
Algebra 1

\cdot		0	1	α	β	
0		0	0	0	0	
1		0	1	α	β	\cdot
α		0	α	β	1	
β		0	β	1	α	

JOUNI PARKKONEN

LUENTOJA JYVÄSKYLÄN YLIOPISTOSSA

TALVELLA JA KEVÄÄLLÄ 2020

Sisältö

I	Laskutoimituksista	1
1	Laskutoimitukset	3
1.1	Laskutoimitus	3
1.2	Indusoitu laskutoimitus	4
1.3	Homomorfismi	5
1.4	Assosiatiivisuus ja kommutatiivisuus	6
1.5	Neutraalialkio	8
1.6	Käänteisalkio	9
1.7	Kompleksiluvut	10
1.8	Potenssit ja monikerrat	12
	Harjoitustehtäviä	13
2	Tekijälaskutoimitus ja modulaariaritmetiikka	17
2.1	Ekvivalenssirelaatio ja kongruenssiluokat	17
2.2	Tekijälaskutoimitus	20
2.3	Kongruenssiluokkien laskutoimitukset	20
	Harjoitustehtäviä	21
II	Renkaat ja kunnat	23
3	Renkaat	25
3.1	Distributiivisuus	25
3.2	Ryhmä	26
3.3	Rengas	27
3.4	Alirengas	29
3.5	Rengashomomorfismit	30
3.6	Renkaan karakteristika	32
	Harjoitustehtäviä	33
4	Kunnat	35
4.1	Yksiköt	35
4.2	Jakorenkaat ja kunnat	36

4.3	Hamiltonin kvaterniot	38
4.4	Lineaarialgebraa	39
	Harjoitustehtäviä	40
5	Jaollisuus	43
5.1	Jaollisuudesta	43
5.2	Jaottomat alkiot ja alkuaalkiot	45
5.3	Renkaan $\mathbb{Z}/q\mathbb{Z}$ yksiköt	46
	Harjoitustehtäviä	47
6	Polynomirenkaat	49
6.1	Polynomit ja polynomifunktiot	49
6.2	Polynomirengas	50
6.3	Polynomien vaihtoehtoinen määritelmä	51
6.4	Aste	52
6.5	Polynomien jakoyhtälö	54
6.6	Polynomien juuret ja jaollisuus	55
6.7	Algebrallisesti suljetut kunnat	57
	Harjoitustehtäviä	58
7	Ideaalit ja kuntalaajennukset	61
7.1	Ideaalit	61
7.2	Tekijärenkaat	64
7.3	Maksimaaliset ideaalit	66
7.4	Kuntalaajennukset polynomirenkaiden avulla	67
	Harjoitustehtäviä	69
III	Ryhmät	71
8	Ryhmät	73
8.1	Ryhmä	73
8.2	Ryhmien suora tulo	77
8.3	Ryhmähomomorfismit	78
8.4	Jäännösluokkien multiplikatiiviset ryhmät	79
	Harjoitustehtäviä	81
9	Aliryhmät	83
9.1	Aliryhmät	83
9.2	Homomorfismin ydin	85
9.3	Osajoukon virittämä aliryhmä	86
9.4	Syklinen ryhmä	88
9.5	Ryhmien sisäinen suora tulo	90
9.6	Lineaarialgebran ryhmiä	91
9.7	Lukuteorian ryhmiä	93
	Harjoitustehtäviä	94
10	Symmetriset ryhmät	97

10.1	Symmetrinen ryhmä S_n	97
10.2	Symmetrisen ryhmän rakenteesta	99
10.3	Cayleyn lause	100
10.4	Permutaation merkki	101
10.5	Alternoiva ryhmä A_n	103
	Harjoitustehtäviä	104
11	Lagrangen lause	107
11.1	Sivuluokat	107
11.2	Aliryhmän indeksi ja Lagrangen lause	109
11.3	Lagrangen lauseen sovelluksia lukuteoriaan	111
	Harjoitustehtäviä	111
12	Normaalit aliryhmät ja tekijäryhmät	113
12.1	Normaalit aliryhmät	113
12.2	Tekijäryhmät	114
12.3	Ryhmien ensimmäinen isomorfismilause	116
12.4	Ryhmien toinen ja kolmas isomorfismilause	118
	Harjoitustehtäviä	119
13	Ryhmät ja geometria	121
13.1	Säännöllisten monikulmioiden symmetrioista	121
13.2	Monitahokkaiden symmetrioista	127
	Harjoitustehtäviä	128
A	Kokonaislukujen jaollisuus	131
	Kirjallisuutta	135

Lukijalle

Tämä teksti on talven ja kevään 2020 kurssien ALGEBRA 1: RENKAAT JA KUNNAT ja ALGEBRA 1: RYHMÄT oppimateriaali. Kurssit muodostavat johdatuksen abstraktiin algebraan, jossa tehdään päätelmiä, kun laskutoimitusten jotkin ominaisuudet tunnetaan. Teoriaa havainnollistetaan useilla esimerkeillä matematiikan eri aloilta (joukko-oppi, lineaarialgebra, analyysi, geometria, lukuteoria).

Yksi algebran keskeinen ajatus on se, että erilaisissa matemaattisissa yhteyksissä tunnistetaan samankaltaisia rakenteita. Jos tunnistetaan jokin tunnettu algebrallinen rakenne (ryhmä, rengas, . . .), voidaan tarkasteltavaa tilannetta usein ymmärtää paremmin näille algebrallisille rakenteille todistettujen yleisten tulosten avulla.

Teksti on jaettu kolmeen osaan ja liitteeseen. Osa I käsittelee laskutoimituksia ja on materiaalia, jota käsitellään molemmilla kursseilla. Osa II muodostaa kurssin RENKAAT JA KUNNAT rungon ja Osa III muodostaa kurssin RYHMÄT rungon. Liitteeseen on koottu kursseilla tarvittavia lukuteorian alkeita, tämä osa on tuttua kurssin Lukuteoria 1 suorittaneille.

Kurssin RENKAAT JA KUNNAT aluksi luvuissa 1–2 tutustutaan laskutoimituksen käsitteeseen ja erilaisiin laskutoimituksiin sekä homomorfismeihin laskutoimituksella varustettujen joukkojen välillä. Luvuissa 3 ja 4 tutustumme renkaisiin ja niiden erityistapauksena kuntiin. Nämä ovat kahdella laskutoimituksella varustettuja joukkoja, jotka yleistävät kokonaislukujen renkaan ja rationaali- ja reaalityönteiden kunnat, joissa laskutoimitukset ovat tavanomaiset yhteen- ja kertolasku. Erityisesti luvussa 6.1 tutustutaan polynomirenkaisiin, jotka ovat kurssilla tärkeässä osassa. Luvussa 5 tarkastelemme jaollisuutta renkaissa ja kurssin huipentumana viimeisessä luvussa tutustutaan ideaaleihin, tekijärenkaisiin ja polynomirenkaiden avulla tehtäviin kuntalajennuksiin. Sovelluksena tarkastelemme äärellisten kuntien konstruktiota.

Kurssin RYHMÄT aluksi tutustutaan laskutoimituksen käsitteeseen ja erilaisiin laskutoimituksiin ja sitten ryhmiin ja niiden välisiin homomorfismeihin. Ryhmät ovat yhdellä laskutoimituksella varustettuja joukkoja, joilla on samoja ominaisuuksia kuin esimerkiksi joukon $\{1, 2, 3\}$ permutaatioiden ryhmällä. Permutaatioryhmiä tarkastellaan yleisessä tapauksessa luvussa 10. Luvussa 11 tutustutaan aliryhmien sivuluokkiin ja todistetaan Lagrangen lause, joka kertoo äärellisen ryhmän aliryhmien mahdolliset koot. Luvussa 12 tutustumme normaaleihin aliryhmiin, määrittelemme laskutoimituksen normaalin aliryhmän sivuluokkien joukossa ja päädyimme tarkastelemaan tärkeää tekijäryhmän käsitettä. Kurssin lopuksi tarkastellaan lyhyesti ryhmäteorian ja geometrian yhteyttä.

Merkintöjä

- $\mathbb{N} = \{0, 1, 2, \dots\}$ luonnolliset luvut.
- $\#(A) \in \mathbb{N} \cup \{\infty\}$ joukon A alkioden lukumäärä.
- $A - B = \{a \in A : a \notin B\}$ joukkojen A ja B erotus.
- $f|_A$ kuvauksen $f: X \rightarrow Y$ rajoittuma osajoukkoon $A \subset X$, $f|_A(a) = f(a)$ kaikilla $a \in A$.
- $\mathcal{F}(X, Y) = \{f: X \rightarrow Y\}$ kaikkien kuvausten $f: X \rightarrow Y$ joukko.
- $\mathcal{F}(X) = (\mathcal{F}(X, X), \circ)$.
- $\bigcup_{\alpha \in A} U_\alpha = \{u : \exists \alpha \in A, \text{ jolle } u \in U_\alpha\}$.
- $\bigcap_{\alpha \in A} U_\alpha = \{u : u \in U_\alpha \text{ kaikilla } \alpha \in A\}$.
- $A \subsetneq B$ joukko A on joukon B aito osajoukko: $A \subset B$ ja $A \neq B$.
- Jos C on matriisi, merkintä C_{lm} tarkoittaa sen lm -kerrointa, joka on rivillä l ja sarakkeessa m .
- $\text{diag}(a_1, a_2, \dots, a_n)$ $n \times n$ -diagonaalimatriisi, jonka diagonaalialkiot ovat a_1, a_2, \dots, a_n .
- $\delta_{mn} = \begin{cases} 1 & \text{jos } m = n \\ 0 & \text{muuten} \end{cases}$.
- $I_n = \text{diag}(1, 1, \dots, 1)$. $(I_n)_{ij} = \delta_{ij}$ kaikilla $i, j \in \{1, 2, \dots, n\}$.
- $\mathbb{R}_+ =]0, \infty[$.
- $\log: \mathbb{R}_+ \rightarrow \mathbb{R}$ on luonnollinen logaritmi.
- ${}^t A$ on matriisin A transpoosi.
- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ on binomikerroin.

Jokaisen luvun lopussa on kokoelma harjoitustehtäviä. Osaan tehtävistä on alaviitteessä numeroitu vihje.

Uusien käsitteiden **määritelmät** on laatikoitu näin. Niitä ei ole numeroitu.

Osa I

Laskutoimituksista

Luku 1

Laskutoimitukset

Tässä luvussa määrittelemme useita kurssin keskeisiä käsitteitä ja tutustumme niiden perusominaisuuksiin.

1.1 Laskutoimitus

Epätyhjän joukon A **laskutoimitus** on kuvaus $*$: $A \times A \rightarrow A$. **Laskutoimituksella varustettu joukko** eli **magma** on pari $(A, *)$, missä $*$ on joukon A laskutoimitus.

Laskutoimituksen tulosta merkitään yleensä $a * a' = *(a, a')$. Laskutoimitus on siis sääntö, joka liittää joukon A alkioiden a ja a' muodostamaan järjestettyyn pariin (a, a') joukon A alkion $a * a'$.

Esimerkki 1.1. Luonnollisten lukujen \mathbb{N} , kokonaislukujen \mathbb{Z} , rationaalilukujen \mathbb{Q} ja reaalilukujen \mathbb{R} yhteen- ja kertolasku ovat laskutoimituksia:

$$(m, n) \mapsto m + n \quad (m, n) \mapsto m \cdot n = mn.$$

Usein laskutoimitukselle ei käytetä mitään erityistä merkkiä vaan laskutoimitusta merkitään kirjoittamalla laskutoimituksella varustetun joukon alkioista muodostettuja “sanoja” kuten tavanomaisessa kertolaskussa on tapana: $a \cdot b = ab$.

Edellä tarkastellut esimerkit liittyvät kaikki tavanomaiseen “luvuilla laskemiseen”. Laskutoimituksen käsite on kuitenkin laajempi, kuten seuraavista esimerkeistä näemme.

Joukon X osajoukot muodostavat **potenssijoukon**

$$\mathcal{P}(X) = \{A : A \subset X\}.$$

Esimerkki 1.2. (a) $\mathcal{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

(b) Joukkojen leikkaus $(A, B) \mapsto A \cap B$ ja yhdiste $(A, B) \mapsto A \cup B$ ovat laskutoimituksia potenssijoukossa $\mathcal{P}(X)$.

(c) Kahden alkion muodostamassa joukossa $X = \{0, 1\}$ on $4^2 = 16$ eri laskutoimitusta: Joukossa

$$X \times X = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

on neljä alkioita ja jokaisella alkiolla on kaksi mahdollista arvoa 0 tai 1.

Esimerkki 1.3. Olkoon $M_n(\mathbb{R})$ reaalisten $n \times n$ -matriisien joukko. Lineaarialgebran kursseilla määritellään kaksi laskutoimitusta joukossa $M_n(\mathbb{R})$. Matriisien yhteenlasku määritellään komponenteittain asettamalla

$$(A + B)_{ij} = (A_{ij} + B_{ij})$$

kaikilla $1 \leq i, j \leq n$. Matriisien kertolasku määritellään asettamalla

$$(AB)_{ij} = \sum_{k=1}^n A_{ik}B_{kj}$$

kaikilla $1 \leq i, j \leq n$.

Erityisesti dimensiossa 2 saadaan laskutoimitukset

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

ja

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

Laskutoimituksella varustetun äärellisen joukon $(X, *)$ **laskutaulu** on joukon X alkiolla indeksoitu taulukko, jossa paikalla (g, h) , siis rivillä g ja sarakkeessa h on alkio gh .

Esimerkki 1.4. Joukon $X = \{0, 1\}$ potenssijoukon laskutoimitusten \cap ja \cup laskutaulut ovat

\cap	\emptyset	$\{0\}$	$\{1\}$	$\{0, 1\}$	ja	\cup	\emptyset	$\{0\}$	$\{1\}$	$\{0, 1\}$
\emptyset	\emptyset	\emptyset	\emptyset	\emptyset		\emptyset	\emptyset	$\{0\}$	$\{1\}$	$\{0, 1\}$
$\{0\}$	\emptyset	$\{0\}$	\emptyset	$\{0\}$		$\{0\}$	$\{0\}$	$\{0\}$	$\{0, 1\}$	$\{0, 1\}$
$\{1\}$	\emptyset	\emptyset	$\{1\}$	$\{1\}$		$\{1\}$	$\{1\}$	$\{0, 1\}$	$\{1\}$	$\{0, 1\}$
$\{0, 1\}$	\emptyset	$\{0\}$	$\{1\}$	$\{0, 1\}$		$\{0, 1\}$	$\{0, 1\}$	$\{0, 1\}$	$\{0, 1\}$	$\{0, 1\}$

1.2 Indusoitu laskutoimitus

Olkoon $(A, *)$ laskutoimituksella varustettu joukko. Jos $B \subset A$, $B \neq \emptyset$ ja kaikille $b, b' \in B$ pätee $b * b' \in B$, niin B on laskutoimituksella varustetun joukon $(A, *)$ **vakaa** osajoukko. Laskutoimitus $*$ määrää **indusoidun laskutoimituksen** $*|_B$ joukossa B , kun asetetaan

$$b * |_B b' = b * b'.$$

Esimerkki 1.5. (a) Rationaalilukujen kertolasku indusoi laskutoimituksen joukkoon $\mathbb{Q} - \{0\}$ ja reaalilukujen kertolasku indusoi laskutoimituksen joukkoon $\mathbb{R} - \{0\}$. Näin saamme laskutoimituksella varustetut joukot $\mathbb{Q}^\times = (\mathbb{Q} - \{0\}, \cdot)$ ja $\mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$.

(b) Olkoon

$$P = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) : c = 0 \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{R}) \right\}.$$

Tällöin kaikille $A, B \in P$ pätee $A + B \in P$ ja $AB \in P$, joten matriisien yhteenlasku ja kertolasku indusoivat kaksi laskutoimitusta joukossa $P \subset M_2(\mathbb{R})$.

Yleensä induoidulle laskutoimitukselle käytetään samaa merkintää kuin laskutoimitukselle, joka indusoi sen: $*|_B = *$.

1.3 Homomorfismi

Kahden laskutoimituksella varustetun joukon väliset kuvaukset, jotka sopivat laskutoimitusten kanssa hyvin yhteen, ovat algebrassa keskeisessä osassa:

Olkoot $(E, *)$ ja (E', \otimes) laskutoimituksella varustettuja joukkoja. Kuvaus $h: (E, *) \rightarrow (E', \otimes)$ on **homomorfismi**, jos $h(a * b) = h(a) \otimes h(b)$ kaikille $a, b \in E$.

- Bijektiivinen homomorfismi on **isomorfismi**.
- Isomorfismi laskutoimituksella varustetulta joukolta E itselleen on **automorfismi**.

Laskutoimituksella varustetut joukot $(E, *)$ ja (E', \otimes) ovat **isomorfisia (keskenään)**, jos on isomorfismi $h: (E, *) \rightarrow (E', \otimes)$.

Lisäksi käytetään melko usein seuraavia nimityksiä: Injektiivinen homomorfismi on **monomorfismi**. Surjektiivinen homomorfismi on **epimorfismi**. Tällä kurssilla käytämme näistä homomorfismityypeistä pääsääntöisesti nimityksiä injektiivinen ja surjektiivinen homomorfismi.

Esimerkki 1.6. (a) Olkoon $n \geq 2$. Lineaarialgebrassa osoitettiin, että kaikille $A, B \in M_n(\mathbb{R})$ pätee

$$\det(AB) = \det A \det B.$$

Siis kuvaus $\det: M_n(\mathbb{R}) \rightarrow (\mathbb{R}, \cdot)$ on homomorfismi.

(b) Yhteenlaskulla varustetut joukot $(M_n(\mathbb{R}), +)$ ja $(\mathbb{R}^{n^2}, +)$ ovat selvästi isomorfisia.

(c) Kuvaus $h: \mathbb{Z} \rightarrow M_2(\mathbb{R})$,

$$h(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

on homomorfismi, kun kokonaisluvut varustetaan yhteenlaskulla ja $M_2(\mathbb{R})$ varustetaan matriisien kertolaskulla:

$$h(n+m) = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = h(n)h(m).$$

Esimerkki 1.7. Reaalilukujen kertolasku indusoi laskutoimituksen positiivisten reaalilukujen joukossa $\mathbb{R}_+ =]0, \infty[$. Eksponenttikuvaus $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot)$, $\exp(x) = e^x$, on homomorfismi: Kaikille $x, y \in \mathbb{R}$ pätee

$$\exp(x + y) = e^{x+y} = e^x e^y = \exp(x) \exp(y).$$

Eksponenttifunktio on tunnetusti bijektio, joten se on isomorfismi. Eksponenttifunktion käänteisfunktio $\log: (\mathbb{R}_+, \cdot) \rightarrow (\mathbb{R}, +)$ on myös isomorfismi: Käänteiskuvauksena se on bijektio ja kaikille $x, y \in \mathbb{R}_+$ pätee

$$\log(xy) = \log(x) + \log(y).$$

Isomorfiset laskutoimituksella varustetut joukot ovat algebrallisilta ominaisuuksiltaan samanlaiset vaikka joukot ja laskutoimitukset voivat “ulkoisesti” olla hyvinkin erilaisia, kuten Esimerkin 1.6 avulla huomaamme.

Propositio 1.8. (1) *Homomorfismien yhdistetty kuvaus on homomorfismi.*

(2) *Isomorfismin käänteiskuvaus on isomorfismi.*

Todistus. (1) Harjoitustehtävä.

(2) Olkoon $\phi: (A, *) \rightarrow (B, \otimes)$ isomorfismi. Olkoot $b_1, b_2 \in B$. Koska ϕ on bijektio, pätee

$$b_1 \otimes b_2 = \phi(\phi^{-1}(b_1)) \otimes \phi(\phi^{-1}(b_2)).$$

Koska ϕ on homomorfismi, saamme

$$\phi(\phi^{-1}(b_1)) \otimes \phi(\phi^{-1}(b_2)) = \phi(\phi^{-1}(b_1) * \phi^{-1}(b_2)).$$

Yhdistämällä nämä kaksi yhtälöä saamme

$$b_1 \otimes b_2 = \phi(\phi^{-1}(b_1) * \phi^{-1}(b_2)),$$

mistä seuraa

$$\phi^{-1}(b_1 \otimes b_2) = \phi^{-1}(b_1) * \phi^{-1}(b_2),$$

koska ϕ on bijektio. Siis ϕ^{-1} on homomorfismi. □

1.4 Assosiatiivisuus ja kommutatiivisuus

Laskutoimitusten suorittamisen järjestyksen kanssa on syytä olla huolellinen. Sulut kertovat, missä järjestyksessä operaatiot suoritetaan: Lausekkeessa $a * (b * c)$ muodostetaan ensin tulo $(b * c)$, joka kerrotaan vasemmalta alkiolla a kun taas lausekkeessa $(a * b) * c$ muodostetaan ensin tulo $(a * b)$, joka kerrotaan oikealta alkiolla c . Nämä eivät välttämättä anna samaa tulosta.

Joukon A laskutoimitus $*$ on

(1) **assosiatiivinen** eli **liitännäinen**, jos $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in A$.

(2) **kommutatiivinen** eli **vaihdannainen**, jos $a * b = b * a$ kaikilla $a, b \in A$.

Sulkujen määrää lausekkeissa voi vähentää, jos laskutoimitus $*$ on assosiativinen: Koska sulkujen paikalla ei ole merkitystä lausekkeessa $a * (b * c) = (a * b) * c$, voimme käyttää merkintää

$$a * b * c = (a * b) * c = a * (b * c)$$

ilman vaaraa. Huomaa kuitenkin, että kaikki laskutoimitukset eivät ole assosiativisia.

Esimerkki 1.9. (a) Luonnollisten lukujen, kokonais-, rationaali- ja reaalilukujen yhteen- ja kertolaskulle pätee

(1) $m + n = n + m$ ja $mn = nm$ kaikilla m, n (kommutatiivisuus).

(2) $m + (n + l) = (m + n) + l$ ja $m(nl) = (mn)l$ kaikilla m, n, l (assosiativisuus).

(b) Kokonaislukujen vähennyslasku ei ole assosiativinen eikä kommutatiivinen:

$$1 - (1 - 1) = 1 \neq -1 = (1 - 1) - 1$$

ja

$$1 - 0 = 1 \neq -1 = 0 - 1.$$

(c) Lineaarialgebran kurssilla on osoitettu, että matriisien yhteen- ja kertolaskut ovat assosiativisia laskutoimituksia joukossa $\text{Mat}_n(\mathbb{R})$. Matriisien yhteenlasku on myös kommutatiivinen mutta matriisien kertolasku joukossa $M_n(R)$ ei ole kommutatiivinen, kun $n \geq 2$. Esimerkiksi

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

(d) Joukon $\mathcal{P}(X)$ laskutoimitukset \cap ja \cup ovat assosiativisia:

$$A \cap (B \cap C) = (A \cap B) \cap C$$

ja

$$A \cup (B \cup C) = (A \cup B) \cup C$$

kaikilla $A, B, C \in \mathcal{P}(X)$, ja kommutatiivisia:

$$A \cap B = B \cap A$$

ja

$$A \cup B = B \cup A$$

kaikilla $A, B \in \mathcal{P}(X)$.

Merkintöjä $+$ ja \cdot käytetään yleisesti eri laskutoimituksille. Merkintää $+$ käytetään kuitenkin ainoastaan kommutatiiviselle laskutoimitukselle.

Seuraava tulos on hyödyllinen luvussa 2 esimerkiksi modulaariaritmetiikan ominaisuuksien perustelussa.

Propositio 1.10. *Olko $h: (E, *) \rightarrow (E', \otimes)$ surjektiivinen homomorfismi.*

(1) Jos $*$ on kommutatiivinen, niin \otimes on kommutatiivinen

(2) Jos $*$ on assosiatiivinen, niin \otimes on assosiatiivinen

Todistus. (1) Olkoot $a', b' \in E'$. Tällöin on $a, b \in E$, joille $h(a) = a'$ ja $h(b) = b'$. Siis

$$a' \otimes b' = h(a) \otimes h(b) = h(a * b) = h(b * a) = h(b) \otimes h(a) = b' \otimes a',$$

joten \otimes on kommutatiivinen.

(2) Harjoitustehtävä 1.10. □

Esimerkki 1.11. Olkoon $X \neq \emptyset$ ja olkoon

$$\mathcal{F}(X) = \{f: X \rightarrow X\}.$$

Kuvausten yhdistäminen \circ on laskutoimitus joukossa $\mathcal{F}(X)$: $(f, g) \mapsto f \circ g$.

Laskutoimitus \circ on assosiatiivinen: Olkoot $f, g, h \in \mathcal{F}(X)$. Yhdistetyn kuvauksen määritelmän mukaan

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

kaikilla $x \in X$ ja

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

kaikilla $x \in X$. Siis $f \circ (g \circ h) = (f \circ g) \circ h$ kaikilla $f, g, h \in \mathcal{F}(X)$.

Laskutoimitus \circ ei ole kommutatiivinen, jos joukossa X on ainakin kaksi alkia: Olkoon $X = \{0, 1\}$ ja olkoot $\underline{0}, \underline{1} \in \mathcal{F}(X)$ vakiokuvaukset $\underline{0}(x) = 0$ ja $\underline{1}(x) = 1$ kaikilla $x \in X$. Tällöin $\underline{1} \circ \underline{0} = \underline{1} \neq \underline{0} = \underline{0} \circ \underline{1}$.

1.5 Neutraalialkio

Olkoon $A \neq \emptyset$ ja olkoon $*$ joukon A laskutoimitus.

- Alkio $e \in A$ on laskutoimituksen $*$ **vasen neutraalialkio**, jos $e * g = g$ kaikilla $g \in A$.
- Alkio $e \in A$ on laskutoimituksen $*$ **oikea neutraalialkio**, jos $g * e = g$ kaikilla $g \in A$.

Jos $e \in A$ on laskutoimituksen $*$ vasen ja oikea neutraalialkio, niin e on laskutoimituksen $*$ **neutraalialkio**.

Esimerkki 1.12. (a) Luku 0 on luonnollisten lukujen, kokonais-, rationaali ja reaalityyppisten lukujen yhteenlaskun neutraalialkio ja luku 1 on kertolaskun neutraalialkio.

(b) Olkoon $X \neq \emptyset$. Määritellään joukon $\mathcal{P}(X)$ laskutoimitus $-$ asettamalla

$$A - B = \{a \in A : a \notin B\}$$

kaikille $A, B \in \mathcal{P}(X)$. Tällöin jokaisella $A \in \mathcal{P}(X)$ pätee $A - \emptyset = A$, joten \emptyset on laskutoimituksen $-$ oikea neutraalialkio. Kuitenkin $\emptyset - A = \emptyset$ kaikilla $A \in \mathcal{P}(X)$, joten \emptyset ei ole laskutoimituksen $-$ vasen neutraalialkio. Vasenta neutraalialkiota ei ole, sillä kaikille $A \in \mathcal{P}(X)$ pätee $A - X = \emptyset \neq X$. Tällä laskutoimituksella ei siis ole neutraalialkiota.

Propositio 1.13. *Olkoon $(X, *)$ laskutoimituksella varustettu joukko. Jos $e \in X$ on laskutoimituksen $*$ vasen neutraalialkio ja $e' \in X$ on laskutoimituksen $*$ oikea neutraalialkio, niin $e = e'$. Erityisesti e on laskutoimituksen $*$ neutraalialkio.*

Todistus. Käyttämällä oletettuja ominaisuuksia ylläolevassa järjestyksessä saadaan $e = e * e' = e'$. Koska e siis toteuttaa ehdot $e * g = g$ ja $g * e = g$ kaikilla $g \in X$, niin e on neutraalialkio. \square

Seuraus 1.14. *Olkoon $(X, *)$ laskutoimituksella varustettu joukko. Jos $e \in X$ on laskutoimituksen $*$ neutraalialkio ja $e' \in X$ on laskutoimituksen $*$ neutraalialkio, niin $e = e'$. \square*

Seurauksen 1.14 tulos voidaan ilmaista lyhyesti näin: Laskutoimituksen neutraalialkio on yksikäsitteinen.

Propositio 1.15. *Olkoon $h: (E, *) \rightarrow (E', \otimes)$ surjektiivinen homomorfismi. Jos laskutoimituksella varustetussa joukossa E on neutraalialkio e , niin $h(e)$ on laskutoimituksella varustetun joukon E' neutraalialkio.*

Todistus. Olkoon $g' \in E'$. Tällöin $g' = h(g)$ jollain $g \in E$ ja pätee

$$h(e) \otimes g' = h(e) \otimes h(g) = h(e * g) = h(g) = g'$$

ja

$$g' \otimes h(e) = h(g) \otimes h(e) = h(g * e) = h(g) = g',$$

joten $h(e)$ on neutraalialkio. \square

Esimerkki 1.16. Helppo esimerkki siitä, että neutraalialkio ei välttämättä kuvaudu neutraalialkiolle, jos homomorfismi ei ole surjektiivinen, on homomorfismi $h: (\mathbb{N}, +) \rightarrow (\mathbb{N}, \cdot)$, $h(n) = 0$ kaikilla $n \in \mathbb{N}$. Kuvaus h on todellakin homomorfismi, koska kaikille $m, n \in \mathbb{N}$ pätee

$$h(n + m) = 0 = 0 \cdot 0 = h(m)h(n).$$

Kuitenkaan neutraalialkio $0 \in (\mathbb{N}, +)$ ei kuvaudu neutraalialkioksi $1 \in (\mathbb{N}, \cdot)$.

1.6 Käänteisalkio

Olkoon $A \neq \emptyset$ ja olkoon $*$ joukon A laskutoimitus, jonka neutraalialkio on e .

- Alkio $\bar{x} \in A$ on alkion $x \in A$ **vasen käänteisalkio**, jos $\bar{x} * x = e$,
- Alkio $\bar{x} \in A$ on alkion $x \in A$ **oikea käänteisalkio**, jos $x * \bar{x} = e$.

Jos \bar{x} on alkion x vasen ja oikea käänteisalkio, niin se on alkion x **käänteisalkio**.

Esimerkki 1.17. Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota laskutoimituksella varustetuissa joukoissa $(\mathbb{N}, +)$ ja (\mathbb{N}, \cdot) . Sen sijaan jokaisella kokonais-, rationaali- ja reaaliluvulla x on vastaluku $-x$, joka on luvun x käänteisalkio yhteenlaskun suhteen.

Luvulla 0 ei ole käänteisalkiota kertolaskun suhteen edes rationaalilukujen joukossa: $0x = x0 = 0 \neq 1$ kaikilla luvuilla x . Kaikilla nollasta poikkeavilla rationaali- ja reaaliluvuilla x sen sijaan on käänteisluku $x^{-1} = 1/x$, esimerkiksi rationaaliluvulle $a/b \neq 0$ pätee $(a/b)^{-1} = b/a$.

Jos laskutoimituksesta käytetään tulomerkintää, neutraalialkiolle käytetään usein merkintää 1 ja summamerkintää käytettäessä merkintää 0. Alkion x käänteisalkiota merkitään yleensä x^{-1} , summamerkintää käytettäessä kuitenkin käytetään merkintää $-x$.

Esimerkki 1.18. (a) Olkoon $X \neq \emptyset$. Identtinen kuvaus $\text{id} = \text{id}_X$ on joukon $\mathcal{F}(X)$ laskutoimituksen \circ neutraalialkio:

$$\text{id} \circ f = f = f \circ \text{id}$$

kaikilla $f \in \mathcal{F}(X)$. Jos $f \in \mathcal{F}(X)$ on bijektio, sen käänteiskuvaus f^{-1} on kuvauksen f käänteisalkio laskutoimituksen \circ suhteen: $f \circ f^{-1} = \text{id} = f^{-1} \circ f$. Muilla joukon $\mathcal{F}(X)$ alkiolla ei ole käänteisalkiota.

(b) Olkoot $f, g \in \mathcal{F}(\mathbb{N})$ kuvaukset, jotka määritellään asettamalla

$$f(n) = \begin{cases} 0, & \text{kun } n = 0 \\ n - 1, & \text{kun } n \neq 0 \end{cases}$$

ja $g(n) = n + 1$. Kuvaukset f ja g eivät ole bijektioita, joten kummallakaan ei ole käänteisalkiota. Kuitenkin pätee $f \circ g = \text{id}$, joten f on kuvauksen g vasen käänteisalkio ja vastaavasti g on kuvauksen f oikea käänteisalkio.

Propositio 1.19. *Olkoon $X \neq \emptyset$ ja olkoon $*$ joukon X assosiativinen laskutoimitus. Jos alkiolla $g \in X$ on käänteisalkio, se on yksikäsitteinen.*

Todistus. Harjoitustehtävä 1.14. □

1.7 Kompleksiluvut

Edellä olemme jo nähneet, että samassa joukossa voi määritellä useita eri laskutoimituksia. Kokonais-, rationaali- ja reaalilukujen aritmetiikkaa yleistettäessä tarkastellaan kahta samassa joukossa määriteltyä laskutoimitusta.

Olkoot $*$ ja \oplus joukon A laskutoimituksia. Kolmikko $(A, *, \oplus)$ on **kahdella laskutoimituksella varustettu joukko**.

Kompleksiluvut $\mathbb{C} = (\mathbb{R}^2, +, \cdot)$ on kahdella laskutoimituksella varustettu joukko, jossa kaikille $(a, b), (c, d) \in \mathbb{R}^2$ asetetaan

$$(a, b) + (c, d) = (a + c, b + d)$$

ja

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

Kompleksiluku $i = (0, 1)$ on **imaginaariyksikkö**.

Huomaa, että kaikille $a, c \in \mathbb{R}$ pätee

$$(a, 0) + (c, 0) = (a + c, 0) \quad \text{ja} \quad (a, 0)(c, 0) = (ac, 0),$$

joten voimme ajatella kompleksilukuja $(a, 0)$ ja $(c, 0)$ reaalilukuina a ja c .

Jokainen kompleksiluku voidaan esittää yksikäsitteisesti summana

$$(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1) = a + ib,$$

jossa käytetään edellä tehtyä sopimusta, jonka mukaan kompleksiluku $(a, 0)$ samastetaan reaaliluvun a kanssa.

Näillä merkinnöillä kompleksilukujen laskutoimitukset ovat

$$\begin{aligned}(a + ib) + (c + id) &= (a + c) + i(b + d), \\ (a + ib)(c + id) &= (ac - bd) + i(ad + bc).\end{aligned}$$

Erityisesti kaikille reaaliluvuille $a \in \mathbb{R}$ ja kompleksiluvuille $c + id$ pätee

$$a(c + id) = (a + i0)(c + id) = ac + iad.$$

Esimerkki 1.20. (a) $i^2 = (0 \cdot 0 - 1 \cdot 1) + i(0 \cdot 1 + 1 \cdot 0) = -1$.

(b) $(1 + i)^2 = (1 \cdot 1 - 1 \cdot 1) + i(1 \cdot 1 + 1 \cdot 1) = 2i$.

Kompleksilukujen kertolaskun lausekkeesta voi tarkastaa, että $zw = 0$, jos ja vain jos $z = 0$ tai $w = 0$. Siis kertolasku indusoi laskutoimituksen joukkoon $\mathbb{C} - \{0\}$ ja saamme laskutoimituksella varustetun joukon $\mathbb{C}^\times = (\mathbb{C} - \{0\}, \cdot)$.

Lemma 1.21. *Kompleksilukujen laskutoimitukset ovat assosiatiivisia ja kommutatiivisia.* □

Olkoot $a, b \in \mathbb{R}$. Kompleksiluvun $z = a + ib$ **reaaliosa** on $\operatorname{Re}(z) = a$, sen **imaginaariosa** on $\operatorname{Im}(z) = b$ ja sen **(kompleksi)konjugaatti** eli **liittoluku** on $\bar{z} = a - ib$.

Kompleksiluvun $z = a + ib$ **(algebra)normi** on

$$\mathbf{n}(z) = z\bar{z} = \operatorname{Re}(z)^2 + \operatorname{Im}(z)^2 \geq 0$$

ja sen **moduli** on

$$|z| = \sqrt{\mathbf{n}(z)} = \|(a, b)\|.$$

On helppo tarkastaa, että jokaisella kompleksiluvulla z on vastaluku $-z = -1z$ ja että jokaisella nollasta poikkeavalla kompleksiluvulla z on käänteisluku

$$z^{-1} = \frac{\bar{z}}{\mathbf{n}(z)}.$$

Jos $x \in \mathbb{R} \subset \mathbb{C}$, niin sen moduli on sama kuin sen itseisarvo reaalilukuna:

$$|x + 0i| = \sqrt{x^2} = |x|.$$

Propositio 1.22. *Kuvaukset $\bar{\cdot}: (\mathbb{C}, +) \rightarrow (\mathbb{C}, +)$ ja $\bar{\cdot}: (\mathbb{C}, \cdot) \rightarrow (\mathbb{C}, \cdot)$ ovat automorfismeja. Kuvaukset $\mathbf{n}, |\cdot|: (\mathbb{C}, \cdot) \rightarrow ([0, \infty[, \cdot)$ ja $\mathbf{n}, |\cdot|: \mathbb{C}^\times \rightarrow (]0, \infty[, \cdot)$ ovat surjektiivisiä homomorfismeja.*

Todistus. Kompleksikonjugoinnin homomorfisuutta koskevat väitteet todistetaan harjoitustehtävässä 1.17. Harjoitustehtävässä 1.17 osoitetaan myös, että kaikille $z \in \mathbb{C}$ pätee $z = \bar{\bar{z}}$, joten $\bar{\cdot}$ on bijektio ja siis automorfismi.

Osoitetaan, että normi on homomorfismi: Olkoot $z, w \in \mathbb{C}$. Normin määritelmän, kompleksikonjugoinnin homomorfisuuden ja kompleksilukujen kertolaskun kommutatiivisuuden ja assosiatiivisuuden nojalla saadaan

$$\mathbf{n}(zw) = (zw)\overline{(zw)} = (zw)(\bar{z}\bar{w}) = (z\bar{z})(w\bar{w}) = \mathbf{n}(z)\mathbf{n}(w),$$

mistä väite seuraa. Vastaava väite modulille seuraa ottamalla neliöjuuri.

Normin ja modulin surjektiivisuus seuraa siitä, että reaaliluvun moduli kompleksilukuna on sama kuin sen itseisarvo. \square

1.8 Potenssit ja monikerrat

Tässä luvussa otamme käyttöön hyödyllisen määritelmän, joka tiivistää merkintöjä.

Olkoon (A, \cdot) assosiatiivisella laskutoimituksella varustettu joukko. Olkoon $a^1 = a$, ja kaikille $n \in \mathbb{N}$, $n \geq 1$ olkoon $a^{n+1} = a^n a$. Jos laskutoimituksella varustetussa joukossa (A, \cdot) on neutraalialkio e , olkoon $a^0 = e$ ja jos alkiolla $a \in A$ on käänteisalkio a^{-1} , olkoon $a^n = (a^{-1})^{-n}$ jokaiselle $n \in \mathbb{Z}$, $n \leq -1$.

Näin määritelty alkio $a^k \in A$ on alkion a **k :s potenssi**.

Jos laskutoimitukselle käytetään yhteenlaskumerkkiä, puhutaan potenssien sijaan monikerroista. Seuraava määritelmä on itse asiassa sama kuin potenssin määritelmä, ero on merkinnässä.

Olkoon $(A, +)$ assosiatiivisella laskutoimituksella varustettu joukko. Olkoon $1 a = a$ ja olkoon $(n + 1)a = na + a$ kaikille $n \in \mathbb{N}$. Jos laskutoimituksella varustetussa joukossa $(A, +)$ on neutraalialkio 0 , olkoon $0 a = 0 \in A$ ja jos alkiolla $a \in A$ on käänteisalkio $-a$ laskutoimituksen $+$ suhteen, olkoon $(-1)a = -a$ ja olkoon $na = (-n)(-a)$ jokaiselle $n \in \mathbb{Z}$, $n \leq -1$.

Näin määritelty alkio $ka \in A$ on alkion a **k :s monikerta**.

Tavanomaiset laskulait pätevät potensseille ja monikerroille:

Lemma 1.23. *Olkoon (A, \cdot) assosiatiivisella laskutoimituksella varustettu joukko, jolla on neutraalialkio. Tällöin*

- (1) $(a^n)^m = a^{nm}$ kaikilla $a \in A$, $n, m \in \mathbb{N}$.
- (2) $a^n a^m = a^{n+m}$ kaikilla $a \in A$, $n, m \in \mathbb{N}$.

Jos alkiolla a on käänteisalkio, niin kohtien (1) ja (2) väitteet pätevät kaikille kokonaisluvuille $m, n \in \mathbb{Z}$.

Olkoon $(H, +)$ kommutatiivisella laskutoimituksella varustettu joukko, jolla on neutraalialkio. Tällöin

- (3) $na + ma = (n + m)a$ kaikilla $a \in H$, $n, m \in \mathbb{N}$.

(4) $n(ma) = (nm)a$ kaikilla $a \in H$, $n, m \in \mathbb{N}$.

Jos alkiolla a on käänteisalkio, niin kohtien (3) ja (4) väitteet pätevät kaikille kokonaisluvuille $m, n \in \mathbb{Z}$.

Todistus. Harjoitustehtävä 1.18. □

Harjoitustehtäviä

1.1. Olkoon

$$\Gamma = \{A \in M_2(\mathbb{R}) : \det A = 1\}.$$

Osoita, että matriisien kertolasku indusoi laskutoimituksen joukossa Γ . Miten matriisien yhteenlasku käyttäytyy?

1.2. Olkoot $(A, *)$ ja (C, \otimes) laskutoimituksella varustettuja joukkoja ja olkoon $f: (A, *) \rightarrow (C, \otimes)$ homomorfismi. Osoita:

(1) Jos $B \subset A$ on vakaa, niin $f(B) \subset C$ on vakaa.

(2) Jos $B \subset C$ on vakaa ja $f^{-1}(B)$ ei ole tyhjä joukko, niin $f^{-1}(B) \subset A$ on vakaa.

1.3. Osoita, että laskutoimituksella varustettu joukko $(\mathbb{R} - \{0\}, \cdot)$ on isomorfinen matriisien kertolaskulla varustetun joukon

$$\left\{ \text{diag}(a, 1/a) : a \in \mathbb{R} - \{0\} \right\} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} : a \in \mathbb{R} - \{0\} \right\}$$

kanssa.

1.4. Olkoot $f: (A, *) \rightarrow (B, \otimes)$ ja $g: (B, \otimes) \rightarrow (C, \cdot)$ laskutoimituksella varustettujen joukkojen homomorfismeja. Osoita, että $g \circ f$ on homomorfismi.

1.5. Olkoon $(A, *)$ laskutoimituksella varustettu joukko ja olkoon $\text{Hom}(A, A)$ kaikkien homomorfismien $\phi: (A, *) \rightarrow (A, *)$ joukko. Osoita, että homomorfismien yhdistäminen on laskutoimitus joukossa $\text{Hom}(A, A)$.

1.6. Ovatko laskutoimituksella varustetut joukot $(\mathcal{P}(\{0, 1\}), \cap)$ ja $(\mathcal{P}(\{0, 1\}), \cup)$ isomorfisia?

1.7. Olkoon X joukko, jossa on ainakin 2 alkia. Onko joukon $\mathcal{P}(X)$ laskutoimitus – assosiatiiivinen?

1.8. Olkoon $*$ kahden alkion joukon $X = \{a, b\}$ laskutoimitus, jonka laskutaulu on

$$\begin{array}{c|cc} * & a & b \\ \hline a & b & b \\ \hline b & a & a \end{array} .$$

Onko laskutoimitus $*$ kommutatiivinen? Onko se assosiatiiivinen?

1.9. Kivi-paperi-sakset -pelissä kaksi pelaajaa näyttää samanaikaisesti kädellään yhden symboleista kivi, paperi tai sakset. Kivi voittaa sakset, sakset voittaa paperin ja paperi voittaa kiven. Jos molemmat pelaajat näyttävät saman symbolin, tämä symboli katsotaan voittajaksi. Pelin sääntö määrää laskutoimituksen kolmen alkion joukolla, jonka alkiot ovat kivi, paperi ja sakset. Muodosta kivi-paperi-sakset -pelin laskutaulu. Onko pelin laskutoimitus assosiatiivinen?

1.10. Olkoot $(E, *)$ ja (E', \otimes) laskutoimituksella varustettuja joukkoja ja olkoon $*$ assosiatiivinen. Olkoon $h: (E, *) \rightarrow (E', \otimes)$ surjektiivinen homomorfismi. Osoita, että \otimes on assosiatiivinen.

1.11. Olkoon $*$ rationaalilukujen laskutoimitus, joka määritellään asettamalla

$$a * b = \frac{a + b}{2}.$$

Onko laskutoimitus $*$ assosiatiivinen? Onko laskutoimituksella $*$ neutraalialkio?

1.12. Olkoon $*$ positiivisten reaalilukujen joukon \mathbb{R}_+ laskutoimitus, joka määritellään asettamalla

$$a * b = \sqrt{ab}.$$

Onko laskutoimitus $*$ assosiatiivinen? Onko laskutoimituksella $*$ neutraalialkio?

1.13. Onko laskutoimituksilla \cap ja \cup neutraalialkiot? Onko jokaisella $A \in \mathcal{P}(X)$ käänteisalkiot laskutoimitusten \cap ja \cup suhteen?

1.14. Todista Propositio 1.19.

1.15. Etsi esimerkki laskutoimituksella varustetusta joukosta $(A, *)$ ja alkioista $a \in A$, jolla on useita vasempia käänteisalkioita.

1.16. Varustetaan luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, 2, \dots\}$ laskutoimituksella \vee , joka määritellään asettamalla

$$a \vee b = \begin{cases} a, & \text{jos } a \geq b \\ b & \text{muuten.} \end{cases}$$

(a) Onko laskutoimitus \vee assosiatiivinen?

(b) Onko laskutoimituksella \vee neutraalialkio?

(c) Millä alkioilla $n \in (\mathbb{N}, \vee)$ on käänteisalkio?

1.17. Osoita, että kaikilla $z, w \in \mathbb{C}$ pätee $\overline{\bar{z}} = z$, $\overline{z + w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$ ja $\mathbf{n}(\bar{z}) = \mathbf{n}(z)$.

1.18. Todista Lemman 1.23 kohtien (1) ja (2) potenssien laskusäännöt.

1.19. Määritellään Harjoitustehtävässä 1.8 käsitellylle laskutoimitukselle $*$ joukon X alkuiden positiiviset potenssit kuten teimme ennen Lemmaa 1.23. Pätevätkö Lemman 1.23 laskusäännöt?

1.20. Varustetaan reaalilukujen joukko \mathbb{R} laskutoimituksella $*$, joka määritellään asettamalla

$$a * b = \sqrt{a^2 + b^2}$$

kaikille $a, b \in \mathbb{R}$.

- (a) Onko laskutoimitus $*$ assosiatiivinen?
- (b) Onko laskutoimituksella $*$ neutraalialkio?

Olkoon $\psi: (\mathbb{R}, *) \rightarrow (\mathbb{R}, +)$ kuvaus, joka määritellään asettamalla $\psi(a) = a^2$ kaikilla $a \in \mathbb{R}$.

- (c) Onko kuvaus $\psi: (\mathbb{R}, *) \rightarrow (\mathbb{R}, +)$ homomorfismi?

Luku 2

Tekijälaskutoimitus ja modulaariaritmetiikka

Tässä luvussa tutustumme ekvivalenssirelaatioon ja määrittelemme, mitä tarkoittaa, että ekvivalenssirelaatio on laskutoimituksen kanssa yhteensopiva. Jos joukossa on määritelty ekvivalenssirelaatio, sen avulla määritellään uusi joukko, ja jos alkuperäisessä joukossa on lisäksi ekvivalenssirelaation kanssa yhteensopiva laskutoimitus, saadaan uuteen joukkoon määriteltyä laskutoimitus, jota sanotaan tekijälaskutoimitukseksi. Tämä konstruktio on tärkeä erityisesti luvussa 7 kurssilla RENKAAT JA KUNNAT ja luvussa 12 kurssilla RYHMÄT. Tärkeänä esimerkkinä tutustumme kongruenssiin $\text{mod } q$ kokonaislukujen joukossa ja sen avulla saataviin yhteen- ja kertolaskun tekijälaskutoimituksiin kongruenssiluokkien joukossa.

2.1 Ekvivalenssirelaatio ja kongruenssiluokat

Olkoon A epätyhjä joukko. Joukon $A \times A$ osajoukko on **relaatio** joukossa A . Jos $R \subset A \times A$ on relaatio, merkitään $a R b$, jos ja vain jos $(a, b) \in R$.

Joukon A relaatio R on

- (1) **refleksiivinen**, jos $a R a$ kaikilla $a \in A$,
- (2) **symmetrinen**, jos $b R a$ kaikilla $a, b \in A$, joille $a R b$,
- (3) **transitiivinen**, jos $a R c$ aina kun $a R b$ ja $b R c$,

Jos relaatio on refleksiivinen, symmetrinen ja transitiivinen, se on **ekvivalenssirelaatio**. Jos R on ekvivalenssirelaatio joukossa A , sanotaan, että joukon A alkiot a ja b ovat **ekvivalentteja**, jos $a R b$.

Ekvivalenssirelaation merkkinä käytetään usein merkkiä \sim .

Toinen tärkeä esimerkki relaatiosta on **osittainen järjestys** \leq , joka on refleksiivinen, transitiivinen ja **antisymmetrinen** (jos $a \leq b$ ja $b \leq a$, niin $a = b$) relaatio.

Olkoon \sim ekvivalenssirelaatio joukossa A . Alkion $a \in A$ **ekvivalenssiluokka** on

$$[a] = \{b \in A : a \sim b\}.$$

Ekvivalenssirelaatiota \sim vastaava joukon A **tekijäjoukko** on

$$A/\sim = \{[a] : a \in A\}.$$

Kuvaus $\pi = \pi_{\sim} : A \rightarrow A/\sim$, $\pi(a) = [a]$, on ekvivalenssirelaatiota \sim vastaava **tekijäkuvaus** eli **luonnollinen kuvaus**.

Alkio $a \in A$ on ekvivalenssiluokkansa $[a]$ **edustaja**.

Lemma 2.1. *Olkoon \sim ekvivalenssirelaatio joukossa A ja olkoot $a, b \in A$. Tällöin $[a] = [b]$ tai $[a] \cap [b] = \emptyset$.*

Todistus. Oletetaan, että $[a] \cap [b] \neq \emptyset$. Tällöin on $x \in [a] \cap [b]$ ja tälle alkiole pätee $a \sim x$ ja $b \sim x$. Ekvivalenssirelaation symmetrisyyden nojalla $x \sim b$, joten transitiivisuuden nojalla $a \sim b$. Siis $b \in [a]$. Olkoon $y \in [b]$. Tällöin $b \sim y$, joten transitiivisuuden nojalla $a \sim y$. Siis $[b] \subset [a]$. Vastaavasti osoitetaan, että $[a] \subset [b]$. \square

Olkoon I epätyhjä **indeksijoukko**. Olkoot A_i , $i \in I$, joukon A epätyhjiä osajoukkoja. Jos

$$A = \bigcup_{i \in I} A_i \tag{2.1}$$

ja kaikille $i \neq j$ pätee $A_i \cap A_j = \emptyset$, niin A on **erillinen yhdiste** joukoista A_i , $i \in I$. Merkitsemme joukkojen A_i , $i \in I$, erillistä yhdistettä

$$A = \bigsqcup_{i \in I} A_i.$$

Jos $A = \bigsqcup_{i \in I} A_i$, niin joukot A_i , $i \in I$ muodostavat joukon A **osituksen**.

Propositio 2.2. *Olkoon \sim ekvivalenssirelaatio joukossa X . Ekvivalenssiluokat määräävät joukon X osituksen:*

$$X = \bigsqcup_{[a] \in X/\sim} [a].$$

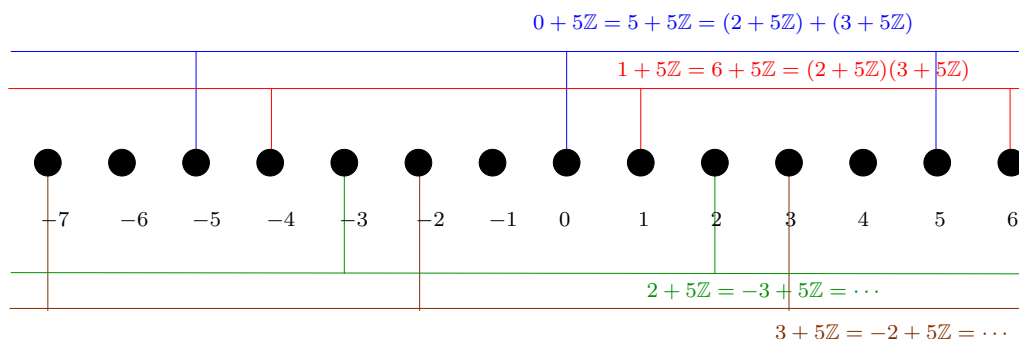
Todistus. Jos $x \in X$, niin $x \in [x]$, joten $X = \bigcup_{[a] \in X/\sim} [a]$. Yhdiste on erillinen Lemman 2.1 nojalla. \square

Joukon A **osituksen** $A = \bigsqcup_{i \in I} A_i$ **määräämä relaatio** R on relaatio, joka määritellään asettamalla $x R y$, jos ja vain jos $x, y \in A_i$ jollain $i \in I$.

Propositio 2.3. *Joukon $X \neq \emptyset$ osituksen määräämä relaatio on ekvivalenssirelaatio.*

Todistus. Olkoon R osituksen $A = \bigsqcup_{i \in I} A_i$ määräämä relaatio. Koska $A = \bigcup_{i \in I} A_i$, niin jokaiselle $a \in A$ pätee $a \in A_i$ jollakin $i \in I$. Siis $a R a$, joten R on refleksiivinen. Relaatio R on symmetrinen, koska $a R b$ määritellään ehdolla $a, b \in A_i$. Oletetaan sitten, että $a, b \in A_i$ ja $c, d \in A_j$ joillain $i, j \in I$. Koska joukot A_k , $k \in I$ muodostavat joukon A osituksen,

pätee joko $A_i = A_j$ tai $A_i \cap A_j = \emptyset$. Oletuksen mukaan $b \in A_i \cap A_j$, joten $A_i = A_j$ ja siis $a, c \in A_i$, joten relaatio R on transitiivinen. \square



Kuva 21: Kongruenssiluokat modulo 5.

Lemma 2.4. *Olkoon $q \in \mathbb{N}$, $q \geq 2$. Olkoon relaatio \equiv joukossa \mathbb{Z} määritelty säännöllä $a \equiv b$, jos on $k \in \mathbb{Z}$ siten, että $b = a + kq$. Tällöin \equiv on ekvivalenssirelaatio.*

Todistus. Tarkastamme, että ekvivalenssirelaation määrittelevät ehdot ovat voimassa

- (1) $a = a + 0q$ kaikilla $a \in \mathbb{Z}$,
- (2) jos $b = a + kq$ jollain $k \in \mathbb{Z}$, niin $a = b + (-k)q$,
- (3) jos $b = a + kq$ ja $c = b + nq$ joillain $k, n \in \mathbb{Z}$, niin $c = a + (k + n)q$. \square

Olkoon $q \in \mathbb{N} - \{0, 1\}$. Ekvivalenssirelaatio \equiv on **kongruenssi (modulo q)**. Tälle ekvivalenssirelaatiolle käytetään merkintää

$$a \equiv b \pmod{q} \quad \text{tai} \quad a \equiv b \pmod{q}.$$

Kongruenssin ekvivalenssiluokat ovat **kongruenssiluokkia (modulo q)**:

$$a + q\mathbb{Z} = \{b \in \mathbb{Z} : b \equiv a \pmod{q}\}.$$

Kongruenssin modulo q tekijäjoukko on

$$\mathbb{Z}/q\mathbb{Z} = \{a + q\mathbb{Z} : a \in \mathbb{Z}\}.$$

Luvun 0 kongruenssiluokkaa voidaan merkitä lyhyesti $0 + q\mathbb{Z} = q\mathbb{Z}$.

Propositio 2.5. *Olkoon $q \in \mathbb{N} - \{0, 1\}$. Tällöin*

$$\mathbb{Z}/q\mathbb{Z} = \{q\mathbb{Z}, 1 + q\mathbb{Z}, 2 + q\mathbb{Z}, \dots, q - 1 + q\mathbb{Z}\}.$$

Todistus. Seuraa jakoyhtälöstä (Propositio A.1): jokaiselle ekvivalenssiluokalle on yksikäsitteinen edustaja joukossa $\{0, 1, \dots, q - 1\}$. \square

2.2 Tekijälaskutoimitus

Joukon A laskutoimitus $*$ ja ekvivalenssirelaatio \sim ovat **yhteensopivat**, jos $a * b \sim a' * b'$ aina kun $a \sim a'$ ja $b \sim b'$.

Lemma 2.6. *Olkoon $(A, *)$ laskutoimituksella varustettu joukko ja olkoon \sim joukon A ekvivalenssirelaatio, joka on yhteensopiva laskutoimituksen $*$ kanssa. Lauseke*

$$[a] * [b] = [a * b]$$

määrittää laskutoimituksen tekijäjoukossa A/\sim .

Todistus. Harjoitustehtävä 2.4. □

Jos joukon A ekvivalenssirelaatio \sim ja laskutoimitus $*$ ovat yhteensopivat, niin Lemman 2.6 antama tekijäjoukon A/\sim laskutoimitus $*$ on joukon A laskutoimituksen $*$ määräämä **tekijälaskutoimitus**.

Seuraavat havainnot seuraavat suoraviivaisesti määritelmistä:

Propositio 2.7. *Olkoon \sim laskutoimituksella varustetun joukon $(E, *)$ laskutoimituksen $*$ kanssa yhteensopiva ekvivalenssirelaatio. Tällöin:*

- (1) *Luonnollinen kuvaus $E \rightarrow E/\sim$ on surjektiivinen homomorfismi.*
- (2) *Jos $e \in E$ on laskutoimituksen $*$ neutraalialkio, niin $[e] \in E/\sim$ on tekijälaskutoimituksen neutraalialkio.*
- (3) *Jos laskutoimitus $*$ on assosiatiivinen, sen tekijälaskutoimitus on assosiatiivinen.*
- (4) *Jos $*$ on kommutatiivinen, sen tekijälaskutoimitus on kommutatiivinen.*

Todistus. Todistetaan väite (1): Kaikille $a, b \in E$ pätee

$$\pi(a) * \pi(b) = [a] * [b] = [a * b] = \pi(a * b),$$

joten luonnollinen kuvaus on homomorfismi. Kuvauksen surjektiivisuus on selvää, koska jokaisella ekvivalenssiluokalla on edustaja joukossa E .

Väite (2) seuraa Propositioista 1.15 ja väitteet (3) ja (4) Propositioista 1.10, koska luonnollinen kuvaus on väitteen (1) mukaan surjektiivinen homomorfismi. □

2.3 Kongruenssiluokkien laskutoimitukset

Lemma 2.8. *Kokonaislukujen yhteenlasku ja kertolasku ovat yhteensopivia kongruenssin kanssa.*

Todistus. Osoitamme väitteen yhteenlaskulle. Kertolaskulle väite osoitetaan samaan tapaan Harjoitustehtävässä 2.1. Jos $a \equiv a' \pmod{q}$ ja $b \equiv b' \pmod{q}$, niin on $m, n \in \mathbb{Z}$, joille $a' = a + mq$ ja $b' = b + nq$. Tällöin

$$a' + b' - (a + b) = (m + n)q,$$

joten $a' + b' \equiv a + b \pmod{q}$. □

Propositio 2.9. (1) Kokonaislukujen yhteenlasku ja kertolasku määräävät assosiatiiviset ja kommutatiiviset laskutoimitukset q alkion joukossa $\mathbb{Z}/q\mathbb{Z}$.

(2) Kongruenssiluokka $0+q\mathbb{Z}$ on kongruenssiluokkien yhteenlaskun neutraalialkio ja $1+q\mathbb{Z}$ on kongruenssiluokkien kertolaskun neutraalialkio.

(3) Jokaisella $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ pätee $a + q\mathbb{Z} + (-a + q\mathbb{Z}) = 0 + q\mathbb{Z}$.

Todistus. Proposition 2.7 nojalla molemmat tekijälaskutoimitukset ovat assosiatiivisia ja kommutatiivisia. Neutraalialkiot saadaan myös Propositioista 2.7. \square

Käytämme molemmille kongruenssiluokkien laskutoimituksille samoja merkintöjä kuin indusoiville laskutoimituksille: kaikille $a + q\mathbb{Z}, b + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$

$$(a + q\mathbb{Z}) + (b + q\mathbb{Z}) = (a + b) + q\mathbb{Z}$$

ja

$$(a + q\mathbb{Z})(b + q\mathbb{Z}) = ab + q\mathbb{Z}.$$

Esimerkki 2.10. Yhteen- ja kertolaskun laskutaulut kongruenssiluokilla modulo 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ja modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Näissä laskutauluissa merkitään luvulla $0 \leq a \leq q-1$ ekvivalenssiluokkaa $a + q\mathbb{Z}$, kun $q \in \{4, 5\}$. Huomaamme, että jokaisella nollasta poikkeavalla alkiolla on käänteisalkio laskutoimituksella varustetussa joukossa $(\mathbb{Z}/5\mathbb{Z}, \cdot)$ mutta ei joukossa $(\mathbb{Z}/4\mathbb{Z}, \cdot)$.

Harjoitustehtäviä

2.1. Osoita, että kokonaislukujen kertolasku on yhteensopiva kongruenssin kanssa.

2.2. Määritellään relaatio \sim joukossa $\mathbb{N} \times \mathbb{N}$ asettamalla $(m, n) \sim (p, q)$, jos ja vain jos $m + q = n + p$. Osoita, että \sim on ekvivalenssirelaatio.¹

2.3. Määritellään laskutoimitus $*$ joukossa $\mathbb{N} \times \mathbb{N}$ asettamalla

$$(m, n) * (p, q) = (mp + nq, mq + np).$$

¹Tehtävä liittyy kokonaislukujen määrittelemiseen luonnollisten lukujen muodollisina erotuksina.

Osoita, että $*$ on yhteensopiva tehtävän 2.2 ekvivalenssirelaation kanssa. Todistuksessa voi käyttää vain luonnollisia lukuja!²

2.4. Todista Lemma 2.6.

2.5. Muodosta yhteen- ja kertolaskun laskutaulut kongruenssiluokilla modulo 2 ja modulo 6.

2.6. Muodosta yhteen- ja kertolaskun laskutaulut kongruenssiluokilla modulo 3 ja modulo 9.

2.7. Määritellään relaatio \sim reaalilukujen joukossa \mathbb{R} asettamalla $x \sim y$, jos ja vain jos $x = qy$ jollain $q \in \mathbb{Q}^\times$. Osoita, että \sim on ekvivalenssirelaatio. Osoita, että tekijäjoukko \mathbb{R}/\sim on ylinumeroituva.

Olkoon $f: X \rightarrow A$ kuvaus. Olkoon $x \sim_f y$, jos ja vain jos $f(x) = f(y)$ alkioille $x, y \in X$.

2.8. Osoita, että \sim_f on ekvivalenssirelaatio. Osoita, että lauseke

$$F([x]) = f(x)$$

määrittelee bijektion $F: X/\sim_f \rightarrow f(X)$.

2.9. Olkoon $\phi: (X, *) \rightarrow (A, \otimes)$ homomorfismi. Osoita, että laskutoimitus $*$ ja ekvivalenssirelaatio \sim_ϕ ovat yhteensopivat. Osoita, että laskutoimitus \otimes indusoi laskutoimituksen joukkoon $\phi(X)$ ja että homomorfismin ϕ määräämä kuvaus $\Phi: X/\sim_\phi \rightarrow \phi(X)$ on isomorfismi.

²Tarkasteltava laskutoimitus antaa kokonaislukujen kertolaskun. Vihje: Osoita, että ehdosta $(m, n) \sim (m', n')$ seuraa $(m, n) * (p, q) \sim (m', n') * (p, q)$ ja päättelee väite käyttämällä ekvivalenssirelaatioiden ja tarkasteltavan laskutoimituksen ominaisuuksia.

Osa II

Renkaat ja kunnat

Luku 3

Renkaat

Renkaat ovat kahdella assosiatiivisella laskutoimituksella varustettuja joukkoja, joissa ainakin toinen laskutoimitus on kommutatiivinen. Vaadimme näiltä kahdella laskutoimituksella varustetuilta joukoilta joitakin samoja ominaisuuksia joita kokonaisluvuilla on, mutta kertolasku ei välttämättä ole kommutatiivinen. Tässä luvussa aloitamme tutustumisen renkaiden perusominaisuuksiin ja eri tapoihin luokitella renkaita ominaisuuksiensa perusteella. Tutkimme myös useita esimerkkejä renkaista.

3.1 Distributiivisuus

Kahdella laskutoimituksella varustettu joukko on niin yleinen käsite, että yhtenäisen teorian esittämiseksi on hyvä edellyttää, että laskutoimitukset sopivat jollain tavalla yhteen keskenään.

Olkoon $(A, *, \oplus)$ kahdella laskutoimituksella varustettu joukko. Laskutoimitus $*$ on **distributiivinen laskutoimituksen \oplus suhteen**, jos

$$\begin{aligned} a * (b \oplus c) &= (a * b) \oplus (a * c) \quad \text{ja} \\ (b \oplus c) * a &= (b * a) \oplus (c * a) \end{aligned} \tag{3.1}$$

kaikilla $a, b, c \in A$.

Distributiivisuuden määritteleviä yhtälöitä (3.1) sanotaan **osittelulaeiksi**.

Esimerkki 3.1. Tunnetusti kaikille luonnollisille luvuille, kokonais-, rationaali- ja reaaliluvuille a, b, c pätee

$$(a + b)c = ac + bc = ca + cb = c(a + b),$$

joten kertolasku on distributiivinen yhteenlaskun suhteen. On myös helppo tarkastaa, että sama pätee kompleksiluvuille. Toisaalta on helppo tarkastaa, että yhteenlasku ei ole distributiivinen kertolaskun suhteen.

Lemma 3.2. *Kongruenssiluokkien kertolasku on distributiivinen yhteenlaskun suhteen.*

Todistus. Olkoot $a, b, c \in \mathbb{Z}$ ja olkoon $q \in \mathbb{N} - \{0, 1\}$. Tällöin kokonaislukujen osittelulain nojalla pätee

$$\begin{aligned} (a + q\mathbb{Z})((b + q\mathbb{Z}) + (c + q\mathbb{Z})) &= (a + q\mathbb{Z})((b + c) + q\mathbb{Z}) = a(b + c) + q\mathbb{Z} \\ &= (ab + ac) + q\mathbb{Z} = (ab + q\mathbb{Z}) + (ac + q\mathbb{Z}). \quad \square \end{aligned}$$

3.2 Ryhmä

Ryhmät ovat pääosassa kurssilla RYHMÄT. Tälläkin kurssilla ryhmän käsite on hyödyllinen käsite renkaiden ja vektoriavaruuksien määritelmässä ja renkaiden teoriassa muutenkin. Tutustumme siksi ryhmän määritelmään ja joihinkin perusominaisuuksiin jo nyt.

Laskutoimituksella varustettu joukko $(G, *)$ on **ryhmä**, jos

- laskutoimitus $*$ on assosiatiivinen,
- laskutoimituksella $*$ on neutraalialkio ja
- jokaisella $g \in (G, *)$ on käänteisalkio.

Esimerkki 3.3. Laskutoimituksella varustetut joukot $(\mathbb{R}, +)$ ja $(\mathbb{Q}, +)$ ryhmiä.

Supistussäännöt ovat voimassa laskutoimituksella varustetussa joukossa $(A, *)$, jos kaikilla $a, b, c \in A$ pätee

- (1) Jos $a * b = a * c$, niin $b = c$.
- (2) Jos $a * b = c * b$, niin $a = c$.

Propositio 3.4. *Supistussäännöt pätevät ryhmässä.*

Todistus. Olkoon G ryhmä ja olkoot $a, b, c \in G$ siten, että $ab = ac$. Siis

$$b = a^{-1}(ab) = a^{-1}(ac) = c,$$

joten sääntö (1) pätee. Sääntö 2 todistetaan samaan tapaan. □

Seuraus 3.5. *Olkoon $(G, *)$ ryhmä. Jokaisella $g \in G$ on täsmälleen yksi käänteisalkio.*

Todistus. Alkiolla $g \in G$ on ainakin yksi käänteisalkio ryhmän määritelmän nojalla. Jos e on ryhmän G neutraalialkio ja $ag = e = bg$, niin supistussäännön nojalla $a = b$. Siis käänteisalkioita on vain yksi.¹ □

Esimerkki 3.6. Supistussääntö ei päde esimerkiksi laskutoimituksella varustetuissa joukoissa (\mathbb{N}, \cdot) ja (\mathbb{R}, \cdot) , koska $0a = 0$ kaikille $a \in \mathbb{N}$. Supistussääntö pätee myös esimerkiksi laskutoimituksella varustetussa joukossa $(\mathbb{N} - \{0\}, \cdot)$, joka ei ole ryhmä.

¹Väite seuraa toki Propositioista 1.19 mutta näin sen saa supistussäännöllä!

Propositio 3.7. Olkoot G ja G' ryhmiä ja olkoon $\phi: G \rightarrow G'$ homomorfismi. Tällöin

(1) Jos $e \in G$ ja $e' \in G'$ ovat ryhmien neutraali-alkiot, niin $\phi(e) = e'$.

(2) $\phi(g^{-1}) = \phi(g)^{-1}$ kaikille $g \in G$.

Todistus. (1) Olkoon $\phi: G \rightarrow G'$ homomorfismi. Tällöin

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e),$$

mistä väite seuraa supistussäännöllä.

(2) Olkoon $g \in G$. Tällöin

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e) = e'$$

ja

$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e',$$

joten $\phi(g^{-1}) = \phi(g)^{-1}$. □

3.3 Rengas

Olkoon $R \neq \emptyset$ joukko, jolla on määritelty kaksi assosiativista laskutoimitusta $+$ ja \cdot . Kolmikko $(R, +, \cdot)$ on **(ykkösellinen) rengas**, jos

- (1) $(R, +)$ on kommutatiivinen ryhmä,
- (2) kertolasku on distributiivinen yhteenlaskun suhteen ja
- (3) kertolaskulla on neutraali-alkio $1 = 1_R \in R$.

Laskutoimituksen $+$ neutraali-alkiolle käytetään merkintää $0 = 0_R$.

Ryhmä $(R, +)$ on renkaan $(R, +, \cdot)$ **additiivinen ryhmä**.

Rengas on **kommutatiivinen rengas**, jos kertolasku on kommutatiivinen.

Jos R on rengas ja $x, y \in R$, niin käytämme tavanomaista merkintää $x - y = x + (-y)$.

Esimerkki 3.8. Lukujen 1, 2.3 ja 3.1 nojalla kahdella laskutoimituksella varustetut joukot $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ ja $(\mathbb{Z}/q\mathbb{Z}, +, \cdot)$, kun $q \in \mathbb{N} - \{0, 1\}$, ovat kommutatiivisia renkaita.

Kun viittaamme renkaseen \mathbb{Z} , \mathbb{Q} , \mathbb{R} , $\mathbb{Z}/q\mathbb{Z}$ tarkoitamme rengasta, jonka laskutoimitukset ovat kuten Esimerkissä 3.8.

Olkoon $q \in \mathbb{N} - \{0, 1\}$. Rengas $\mathbb{Z}/q\mathbb{Z}$ on **jäännösluokkarengas** mod q .

Esimerkki 3.9. Olkoon $X \neq \emptyset$ ja olkoon R rengas. Olkoon $\mathcal{F}(X, R)$ joukko, joka koostuu kaikista kuvauksista joukolta X renkaaseen R . Määritellään tässä joukossa yhteen- ja kertolasku pisteittäin: Olkoot $f, g \in \mathcal{F}(X, R)$. Asetamme

$$(f + g)(x) = f(x) + g(x) \quad \text{ja} \quad (fg)(x) = f(x)g(x)$$

kaikilla $x \in X$. Joukko $\mathcal{F}(X, R)$ varustettuna näillä laskutoimituksilla on rengas, jota kutsutaan **funktio renkaaksi**.

Laskutoimitusten assosiativisuus, yhteenlaskun kommutatiivisuus ja kertolaskun distributiivisuus yhteenlaskun suhteen seuraa siitä, että funktioiden arvot ovat renkaassa R ja funktioiden laskutoimitukset on määritelty pisteittäin. Yhteenlaskun (vastaavasti kertolaskun) neutraali alkio on vakiofunktio $0: X \rightarrow R$ (vastaavasti $1: X \rightarrow R$). Funktion $f \in \mathcal{F}(X, R)$ käänteisalkio yhteenlaskun suhteen on funktio $-f$, joka määritellään asettamalla $(-f)(x) = -f(x)$ kaikilla $x \in R$.

Rengas $\mathcal{F}(X, R)$ on kommutatiivinen, jos R on kommutatiivinen. Esimerkiksi siis $\mathcal{F}(\mathbb{R}, \mathbb{R})$ on kommutatiivinen rengas.

(d) Olkoot $L_1, L_2: \mathbb{R}^n \rightarrow \mathbb{R}^n$ lineaarikuvauksia. Lineaarialgebran kurssilla on osoitettu, että $L_1 + L_2$ ja $L_1 \circ L_2$ ovat myös lineaarikuvauksia avaruudelta \mathbb{R}^n itselleen. Vektoriarvuuden \mathbb{R}^n **endomorfismirengas** on

$$\text{End}(\mathbb{R}^n) = \{L: \mathbb{R}^n \rightarrow \mathbb{R}^n : L \text{ on lineaarikuvaus}\}$$

varustettuna yhteenlaskulla

$$(L_1 + L_2)(x) = L_1(x) + L_2(x)$$

kaikilla $x \in \mathbb{R}^n$ ja kertolaskulla

$$L_1 L_2 = L_1 \circ L_2.$$

Molemmat laskutoimitukset ovat assosiativisia² ja yhteenlasku on kommutatiivinen.

Lineaarikuvaus $0 \in \text{End}(\mathbb{R}^n)$ on selvästi yhteenlaskun neutraali alkio. Määritellään jokaiselle $L \in \text{End}(\mathbb{R}^n)$ lineaarikuvaus $-L \in \text{End}(\mathbb{R}^n)$ asettamalla $(-L)(x) = -L(x)$ kaikilla $x \in \mathbb{R}^n$. Tällöin selvästi $L + (-L) = 0$ kaikilla $L \in \text{End}(\mathbb{R}^n)$, joten $(\text{End}(\mathbb{R}^n), +)$ on kommutatiivinen ryhmä.

Jos $L, L', L'' \in \text{End}(\mathbb{R}^n)$, niin kaikilla $a \in \mathbb{R}^n$ pätee

$$(L + L')L''(a) = LL''(a) + L'L''(a) = (LL'' + L'L'')(a),$$

ja

$$L''(L + L')(a) = L''(L(a) + L'(a)) = L''L(a) + L''L'(a) = (L''L + L''L')(a).$$

Siis kertolasku on yhteenlaskun suhteen distributiivinen.

Lisäksi identtinen kuvaus $\text{id}: \mathbb{R}^n \rightarrow \mathbb{R}^n$ on lineaarikuvaus ja se on selvästi kertolaskun neutraali alkio, joten $\text{End}(\mathbb{R}^n)$ on rengas.

Propositio 3.10. *Olkoon R rengas. Tällöin*

- (1) $0_R \cdot x = 0_R = x \cdot 0_R$ kaikilla $x \in R$,
- (2) $x(-y) = (-x)y = -(xy)$ ja $(-x)(-y) = xy$ kaikilla $x, y \in R$,
- (3) $x(y - z) = xy - xz$ ja $(y - z)x = yx - zx$ kaikilla $x, y, z \in R$,

²Katso Esimerkki 1.11.

Todistus. (1) Distributiivisuuden nojalla

$$0_R x + x = (0_R + 1_R)x = 1_R x = x$$

kaikilla $x \in R$. Toinen yhtälö todistetaan samalla tavalla. Renkaan R additiivisen ryhmän supistussäännöstä seuraa, että $0_R x = 0_R$ kaikilla $x \in R$.

Loput väitteet todistetaan harjoitustehtävässä 3.4. □

Esimerkki 3.11. Renkaassa R pätee $-1_R x = -x$ kaikilla $x \in R$.

Edellä osoitettujen laskusääntöjen avulla on helppo osoittaa seuraavat perusominaisuudet

Propositio 3.12. *Olkoon R rengas. Jos $\#R \geq 2$, niin*

(1) $0 \neq 1$ ja

(2) yhteenlaskun neutraalialkiolla 0 ei ole käänteisalkiota kertolaskun suhteen.

Todistus. (1) Jos $1 = 0$, niin kaikille $x \in R$ pätee Proposition 3.10 nojalla

$$x = 1x = 0x = 0.$$

Toinen väite todistetaan harjoitustehtävänä 4.1. □

Esimerkki 3.13. Olkoon R rengas, jossa on vähintään 2 alkioita. Kaikkien R -kertoimisten $n \times n$ -matriisien joukko $M_n(R)$ varustettuna matriisien yhteen- ja kertolaskulla on rengas. Kun $R = \mathbb{R}$, kaikki renkaan ominaisuudet on osoitettu lineaarialgebrassa, katso Esimerkit 1.3 ja 3.1(b). Kun $n \geq 2$, niin $M_n(R)$ ei ole kommutatiivinen rengas, koska matriisien kertolasku ei ole kommutatiivinen:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Lemma 3.14. *Kommutatiivisessa renkaassa K pätee binomikaava:*³

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

kaikille $a, b \in K$ ja kaikille $n \in \mathbb{N}$.

Todistus. Harjoitustehtävä 3.5. □

3.4 Alirengas

Olkoon R rengas ja olkoon $S \subset R$ vakaa yhteenlaskun ja kertolaskun suhteen. Jos S varustettuna indusoiduilla laskutoimituksilla on rengas ja jos $1_S = 1_R$, niin S on renkaan R alirengas.

³Katso monikerran ja potenssin määritelmä luvusta 1.8.

Esimerkki 3.15. Joukko

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

on rengas renkaasta $M_2(\mathbb{R})$ indusoiduilla laskutoimituksilla. Sen kertolaskun neutraali-alkio on $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, joten S ei ole renkaan $M_2(\mathbb{R})$ alirengas.

Esimerkki 3.15 osoittaa, että oletus $1_S = 1_R$ on oleellinen alirenkaan määritelmässä. Sen sijaan alirenkaan yhteenlaskun neutraali-alkio on automaattisesti sama kuin koko renkaan yhteenlaskun neutraali-alkio.

Lemma 3.16. *Olkoon S renkaan R alirengas. Tällöin $0_S = 0_R$.*

Todistus. Neutraali-alkioiden määritelmän nojalla pätee $0_S + 0_S = 0_S = 0_S + 0_R$. Supistussäännön nojalla siis $0_S = 0_R$. \square

Propositio 3.17 (Alirengastesti). *Olkoon R rengas ja olkoon $S \subset R$. Tällöin S on renkaan R alirengas, jos ja vain jos*

- (1) Kaikille $x, y \in S$ $x + y \in S$ ja $xy \in S$ ja
- (2) $-1_R \in S$.

Todistus. Harjoitustehtävä 3.7. \square

Esimerkki 3.18. (a) \mathbb{Z} on renkaan \mathbb{Q} alirengas.

(b)

$$C = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in \mathbb{R} \right\}$$

on renkaan $M_2(\mathbb{R})$ alirengas.

Esimerkki 3.19. Analyysin kursseilla osoitetaan, että indusoiduilla laskutoimituksilla varustetut joukot

$$C^0(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} : f \text{ on jatkuva}\}, \text{ ja}$$

$$C^k(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} : f \text{ on } k \text{ kertaa jatkuvasti derivoituva}\}, \quad k \in (\mathbb{N} - \{0\}) \cup \{\infty\}.$$

ovat funktiorengaan $\mathcal{F}(\mathbb{R}, \mathbb{R})$ alirenkaita

3.5 Rengashomomorfismit

Olkoot R ja R' renkaita. Kuvaus $\phi: R \rightarrow R'$ on **rengashomomorfismi**, jos

- $\phi: (R, +) \rightarrow (R', +)$ on homomorfismi,
- $\phi: (R, \cdot) \rightarrow (R', \cdot)$ on homomorfismi ja
- $\phi(1) = 1$.

Bijektiivinen rengashomomorfismi on **rengasisomorfismi**.

Lemma 3.20. *Rengashomomorfismi kuvaa nollan nolllaksi.*

Todistus. Nolla on additiivisen ryhmän neutraalialkio, joten väite seuraa Propositioista 3.7. \square

Huomaa, että Proposition 3.12 nojalla rengashomomorfismille $\phi: R \rightarrow R'$ pätee $\phi(1) = 0$ vain, jos $R' = \{0\}$. Lisäksi yhden alkion renkaalta ei ole rengashomomorfismia renkaaseen, jossa on vähintään kaksi alkioita.

Esimerkki 3.21. (a) Luonnollinen kuvaus $k \mapsto k + q\mathbb{Z}$ renkaasta $(\mathbb{Z}, +, \cdot)$ jäännösluokarenkaaseen $(\mathbb{Z}/q\mathbb{Z}, +, \cdot)$ on surjektiivinen rengashomomorfismi.

(b) Olkoon X epätyhjä joukko ja olkoon R rengas. Olkoon $a \in X$. **Evaluatiokuvaus** $E_a: \mathcal{F}(X, R) \rightarrow R$, $E_a(f) = f(a)$, on rengashomomorfismi:

$$\begin{aligned} E_a(f + g) &= (f + g)(a) = f(a) + g(a) = E_a(f) + E_a(g), \\ E_a(fg) &= (fg)(a) = f(a)g(a) = E_a(f)E_a(g) \end{aligned}$$

ja

$$E_a(\underline{1}) = \underline{1}(a) = 1.$$

(c) Olkoon $K = \{v_1, v_2, \dots, v_n\}$ vektoriavaruuden \mathbb{R}^n kanta ja olkoon $(Lv_i)_K \in \mathbb{R}^n$ vektorin Lv_i koordinaattivektori sarakevektorina kannassa K . Lineaarialgebrassa on osoitettu, että kuvaus $\text{Mat}: \text{End}(\mathbb{R}^n) \rightarrow M_n(\mathbb{R})$, joka liittyy lineaarikuvaukseen L sen matriisiin tässä kannassa, on rengasisomorfismi. Jos $L, L' \in \text{End}(\mathbb{R}^n)$, niin $(L + L')(v) = Lv + L'v$, joten

$$\text{Mat}(L + L') = \text{Mat}(L) + \text{Mat}(L'),$$

eli Mat on ryhmähomomorfismi additiivisten ryhmien välillä. Lisäksi kaikille lineaarikuvauksille $L, L' \in \text{End}(\mathbb{R}^n)$ pätee

$$\text{Mat}(L'L) = \text{Mat}(L')\text{Mat}(L)$$

ja identtisen kuvauksen matriisi on I_n .

Propositio 3.22. (1) Jos $f: R \rightarrow S$ ja $g: S \rightarrow T$ ovat rengashomomorfismeja, niin $g \circ f$ on rengashomomorfismi.

(2) Rengashomomorfismi $f: R \rightarrow S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi $\bar{f}: S \rightarrow R$, jolle $\bar{f} \circ f = \text{id}_R$ ja $f \circ \bar{f} = \text{id}_S$.

Todistus. Harjoitustehtävät 1.4 ja 3.11. \square

Rengashomomorfismin $\psi: R \rightarrow R'$ **ydin** on

$$\ker \psi = \psi^{-1}(0) = \{x \in R : \psi(x) = 0\}.$$

Propositio 3.23. *Rengashomomorfismi on injektio, jos ja vain jos sen ydin on $\{0\}$.*

Todistus. Olkoon $\psi: S \rightarrow S$ rengashomomorfismi. Koska $\psi(0) = 0$, $0 \in \ker \psi$. Jos ydin ei ole $\{0\}$, on $x \in R - \{0\}$, jolle $\psi(x) = 0 = \psi(0)$. Siis ψ ei ole injektio. Jos taas ψ ei ole injektio, on $x, y \in R$, $x \neq y$, joille $\psi(x - y) = \psi(x) - \psi(y) = 0$. Koska $x - y \neq 0$, pätee $\ker \psi \neq \{0\}$. \square

Esimerkki 3.24. (a) Luonnollisen rengashomomorfismin $\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$, $a \mapsto a + q\mathbb{Z}$, ydin on $q\mathbb{Z}$ kaikilla $q \geq 2$.

(b) Inklusiomorfismi $\mathbb{Z} \rightarrow \mathbb{Q}$, $k \mapsto k$, on injektio. Sen ydin on $\{0\}$.

Rengashomomorfismin ydin ei yleensä ole määrittelyrenkaansa alirengas, kuten tarkastelemamme esimerkitkin osoittavat.

Esimerkki 3.25. Olkoon S renkaan R alirengas. Alirenkään määritelmän mukaan alirenkään inklusiokuvaus $i: S \rightarrow R$, $i(s) = s$, on rengashomomorfismi.

Seuraava tulos yleistää edellisen havainnon.

Propositio 3.26. *Olkoon $\phi: R \rightarrow R'$ rengashomomorfismi.*

(1) *Jos S on renkaan R alirengas, niin $\phi(S)$ on renkaan R' alirengas.*

(2) *Jos S' on renkaan R' alirengas, niin $\phi^{-1}(S')$ on renkaan R alirengas.*

Todistus. (1) Sovelletaan Propositiota 3.17. Olkoot $\phi(a), \phi(b) \in \phi(S)$. Tällöin

$$\phi(a) + \phi(b) = \phi(a + b) \in \phi(S)$$

ja

$$\phi(a)\phi(b) = \phi(ab) \in \phi(S),$$

koska $\phi: (R, +) \rightarrow (R', +)$ ja $\phi: (R, \cdot) \rightarrow (R', \cdot)$ ovat homomorfismeja. Koska $-1_R \in S$, niin Proposition 3.7 kohdan (2) nojalla

$$-1_{R'} = -\phi(1_R) = \phi(-1_R) \in \phi(S).$$

Siis $\phi(S)$ on alirengas.

(2) Harjoitustehtävä 3.12. □

Seuraus 3.27. *Olkoon $\phi: R \rightarrow R'$ rengashomomorfismi. Tällöin $\phi(R)$ on renkaan R' alirengas ja $\phi^{-1}(R')$ on renkaan R alirengas.* □

3.6 Renkaan karakteristika

Kokonaislukujen renkaan \mathbb{Z} rakenne on yksinkertainen: sen kaikki alkioit ovat alkion 1 monikertoja. Tästä seuraa erityisominaisuus renkaassa \mathbb{Z} määritellyille rengashomomorfismeille.

Propositio 3.28. *Olkoon R rengas. On täsmälleen yksi rengashomomorfismi $\phi: \mathbb{Z} \rightarrow R$.*

Todistus. Kuvaus $\phi: \mathbb{Z} \rightarrow R$,

$$\phi(n) = n1_R = 1_R + 1_R + \cdots + 1_R,$$

on rengashomomorfismi, sillä

$$\phi(m + n) = (m + n)1_R = m1_R + n1_R = \phi(m) + \phi(n)$$

ja

$$\phi(mn) = mn1_R = m1_R n1_R = \phi(m)\phi(n).$$

Siis haluttuja kuvauksia on ainakin yksi.

Jos $\psi: \mathbb{Z} \rightarrow R$ on rengashomomorfismi, niin $\psi(1) = 1_R$. Siis $\psi(m) = m\psi(1_R)$, joten $\psi = \phi$. □

Esimerkki 3.29. Olkoon R rengas ja olkoon $\psi: \mathbb{Z} \rightarrow R$ rengashomomorfismi $\psi(k) = k1_R$. Homomorfismin ψ kuva $\psi(\mathbb{Z}) = \{k1_R : k \in \mathbb{Z}\}$ on renkaan R alirengas. Tämä on helppo tarkastaa Proposition 3.17 tai Proposition 3.26 avulla.

Olkoon R rengas. Jos homomorfismi $\mathbb{Z} \rightarrow R, k \mapsto k1_R$, on injektio, niin renkaan R karakteristika $\chi(R)$ on 0. Muuten renkaan R karakteristika on

$$\chi(R) = \min\{k \in \mathbb{N} - \{0\} : k1_R = 0\}.$$

Esimerkki 3.30. (1) Renkaiden $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ karakteristika on 0, koska ne sisältävät kaikki alirenkana isomorfisen kopion kokonaislukurenkaasta \mathbb{Z} .

(2) Jäännösluokkarenkaan $\mathbb{Z}/q\mathbb{Z}$ karakteristika on q .

Lemma 3.31. Jos renkaan R karakteristika on q , niin $qx = 0_R$ kaikille $x \in R$.

Todistus. Harjoitustehtävä 3.13 □

Harjoitustehtäviä

3.1. Onko joukon $\mathcal{P}(X)$ laskutoimitus \cap distributiivinen laskutoimituksen \cup suhteen? Onko laskutoimitus \cup distributiivinen laskutoimituksen \cap suhteen?

Avaruuden \mathbb{R}^3 vektoritulo eli ristitulo on laskutoimitus, joka määritellään asettamalla kaikille $a = (a_1, a_2, a_3)$ ja $b = (b_1, b_2, b_3) \in \mathbb{R}^3$

$$a \times b = \left(\det \begin{pmatrix} a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}, -\det \begin{pmatrix} a_1 & b_1 \\ a_3 & b_3 \end{pmatrix}, \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \right).$$

3.2. Osoita, että

- (1) \times on antikommutatiivinen: $b \times a = -a \times b$ kaikille $a, b \in \mathbb{R}^3$.
- (2) \times on distributiivinen vektorien komponenteittaisen yhteenlaskun suhteen.
- (3) \times ei ole assosiativinen. ⁴

3.3. Määritellään joukossa \mathbb{Z}^3 yhteenlasku komponenteittain ja kertolasku asettamalla

$$(a, b, c)(x, y, z) = (ax, bx + cy, cz)$$

kaikilla $(a, b, c), (x, y, z) \in \mathbb{Z}^3$. Onko \mathbb{Z}^3 varustettuna näillä laskutoimituksilla rengas? Onko se kommutatiivinen?

3.4. Olkoon R rengas. Osoita, että

- (1) $x(-y) = (-x)y = -(xy)$ kaikilla $x, y \in R$,
- (2) $x(y - z) = xy - xz$ ja $(y - z)x = yx - zx$ kaikilla $x, y, z \in R$.

⁴Keksi sopiva esimerkki.

3.5. Todista Lemma 3.14.

3.6. Olkoon (R, \oplus, \cdot) kahdella laskutoimituksella varustettu joukko siten, että

- (1) (R, \oplus) on ryhmä,
- (2) kertolasku on distributiivinen yhteenlaskun suhteen ja
- (3) kertolaskulla on neutraalialkio $1 = 1_R \in R$.

Osoita, että (R, \oplus, \cdot) on rengas.⁵

3.7. Todista Propositio 3.17.

3.8. Olkoot $f: R \rightarrow S$ ja $g: S \rightarrow T$ rengashomomorfismeja. Osoita, että $g \circ f$ on rengashomomorfismi.

3.9. Osoita, että Esimerkin 3.18 (b) rengas C on isomorfinen kompleksilukujen renkaan \mathbb{C} kanssa. Mikä renkaan C kuvaus vastaa kompleksikonjugointia?

3.10. Ovatko funktiorengaat $\mathcal{F}([0, 1], \mathbb{R})$ ja $\mathcal{F}([0, 2], \mathbb{R})$ isomorfisia?

3.11. Todista Propositio 3.22(2).

3.12. Todista Propositio 3.26(2).

3.13. Todista Lemma 3.31.

3.14. Osoita, että renkaalla \mathbb{Z} ei ole muita alirenkaita kuin \mathbb{Z} .

3.15. Olkoon $q \in \mathbb{N} - \{0, 1\}$. Osoita, että ei ole rengashomomorfismia jäännösluokkarenkaalta $\mathbb{Z}/q\mathbb{Z}$ renkaaseen \mathbb{Z} .

3.16. Sievennä lauseke $(a + b)^p$ kommutatiivisessa renkaassa, jonka karakteristika on alkuluku p . Miksi oletamme, että p on alkuluku?

3.17. Olkoon K kommutatiivinen rengas, jonka karakteristika on alkuluku p . Olkoon $\phi: K \rightarrow K$ kuvaus $\phi(a) = a^p$. Osoita, että ϕ on rengashomomorfismi.

⁵Tehtävässä ei oleteta, että \oplus on kommutatiivinen. Tarkastele lauseketta $(1 \oplus 1)(x \oplus y)$.

Luku 4

Kunnat

Tässä luvussa tarkastelemme renkaita, joiden kaikilla nollasta poikkeavilla alkioilla on käänteisalkio kertolaskun suhteen.

4.1 Yksiköt

Jos R on rengas ja alkioilla $u \in R$ on käänteisalkio kertolaskun suhteen, niin u on renkaan R yksikkö.

Propositio 4.1. *Renkaan yksiköiden joukko varustettuna kertolaskulla on ryhmä.*

Todistus. Renkaan R kertolasku on assosiatiiivinen laskutoimitus, jonka neutraalialkio on 1. Yksiköiden joukko on vakaa kertolaskun suhteen: Jos u ja v ovat yksiköitä, niin uv on yksikkö, koska

$$(uv)(v^{-1}u^{-1}) = 1 = (v^{-1}u^{-1})(uv).$$

Kertolasku on siis assosiatiiivinen laskutoimitus yksiköiden joukossa. Laskutoimituksella on neutraalialkio, koska 1 on yksikkö. Määritelmän mukaan jokaisella yksiköllä u on käänteisalkio u^{-1} renkaassa R . Myös u^{-1} on yksikkö, koska $(u^{-1})^{-1} = u$. \square

Renkaan R yksiköiden ryhmä (tai multiplikatiivinen ryhmä) on

$$R^\times = \{u \in R : u \text{ on yksikkö}\}$$

varustettuna renkaan R kertolaskun indusoimalla laskutoimituksella.

Esimerkki 4.2. (a) Jos renkaassa on ainakin kaksi alkioita, niin Proposition 3.12 mukaan $0 \neq 1$ ja 0 ei ole yksikkö.

(b) Renkaissa \mathbb{Q} ja \mathbb{R} kaikki nollasta poikkeavat alkioit ovat yksiköitä, joten aiemmin esitellyt multiplikatiiviset ryhmät \mathbb{Q}^\times ja \mathbb{R}^\times sopivat yhteen yksiköiden ryhmän määritelmän kanssa.

(c) Kokonaislukujen renkaan yksiköiden ryhmä on $\mathbb{Z}^\times = \{-1, 1\}$.

(d) Funktiorenkaan $\mathcal{F}(X, R)$ alkio f on yksikkö, jos ja vain jos $f(X) \subset R^\times$.

4.2 Jakorengaat ja kunnat

Olkoon K rengas, jossa on ainakin kaksi alkioita. Jos kaikki renkaan K nollassa poikkeavat alkioita ovat yksiköitä, niin K on **jakorengas**.

Kommutatiivinen jakorengas on **kunta**.

Jakorengas, joka ei ole kunta on **vinokunta**.

Jos K ja K' ovat kuntia, rengashomomorfismi $\phi: K \rightarrow K'$ on **kuntahomomorfismi**.

Esimerkki 4.3. (a) Renkaassa \mathbb{Z} on äärettömän monta alkioita mutta sen ainoat yksiköt ovat ± 1 . Siis \mathbb{Z} ei ole jakorengas eikä siis kunta.

(b) \mathbb{Q} , \mathbb{R} ja \mathbb{C} ovat kuntia.

(c) Olkoon R rengas, jossa on vähintään kaksi alkioita. Matriisirengas $M_n(R)$ ei ole jakorengas, kun $n \geq 2$, koska esimerkiksi matriisilla A , jonka ainoa nollassa poikkeava kerroin on A_{11} ei ole kääntämismatriisia.

Propositio 4.4. \mathbb{C} on kunta ja kuvaus $j: \mathbb{R} \rightarrow \mathbb{C}$, $j(x) = x$, on kuntahomomorfismi.

Todistus. Seuraa Luvun 1.7 tuloksista. □

Kunnan K alirengas k , joka on kunta, on kunnan K **alikulunta**. Tällöin kunta K on kunnan k **kuntalaajennus**.

Esimerkki 4.5. \mathbb{Q} on kunnan \mathbb{R} alikulunta.

Esimerkki 4.6. Olkoon $F = \{0, 1, \alpha, \beta\}$ joukko, jossa on määritelty kaksi laskutoimitusta $+$ ja \cdot , joiden laskutaulut ovat

$$\begin{array}{c|cccc}
 + & 0 & 1 & \alpha & \beta \\
 \hline
 0 & 0 & 1 & \alpha & \beta \\
 1 & 1 & 0 & \beta & \alpha \\
 \alpha & \alpha & \beta & 0 & 1 \\
 \beta & \beta & \alpha & 1 & 0
 \end{array}
 \quad \text{ja} \quad
 \begin{array}{c|cccc}
 \cdot & 0 & 1 & \alpha & \beta \\
 \hline
 0 & 0 & 0 & 0 & 0 \\
 1 & 0 & 1 & \alpha & \beta \\
 \alpha & 0 & \alpha & \beta & 1 \\
 \beta & 0 & \beta & 1 & \alpha
 \end{array}$$

Laskutaulusta on helppo tarkastaa, että F on kunta. Sen osajoukko $\{0, 1\}$ on vakaa yhteenlaskun ja kertolaskun suhteen ja $-1 = 1$, joten Proposition 3.17 nojalla $\{0, 1\}$ on kunnan F alikulunta.

Propositio 4.7. Olkoon K kunta. Osajoukko $K' \subset K$ on alikulunta, jos ja vain jos

(1) $\#K' \geq 2$,

(2) $a - b \in K'$ kaikilla $a, b \in K'$ ja

(3) $ab^{-1} \in K'$ kaikilla $a, b \in K'$, $b \neq 0$.

Todistus. Oletetaan ensin, että K' on alikulunta. Tällöin se on erityisesti kunta, joten joukossa K' on ainakin kaksi alkioita. Koska $(K', +)$ on ryhmä, saadaan $a - b \in K'$ kaikilla $a, b \in K'$. Vastaavasti $(K')^\times$ on ryhmä Proposition 4.1 nojalla, joten $ab^{-1} \in K'$ kaikilla $a, b \in K', b \neq 0$.

Oletetaan sitten, että osajoukolla K' on ominaisuudet (1)–(3). Oletuksen (2) nojalla kaikille $a \in K'$ pätee $0_K = a - a \in K'$, joten $-a = 0_K - a \in K'$ ja kaikille $a, b \in K'$ pätee $a + b = a - (-b) \in K'$. Vastaavalla tavalla saadaan oletuksesta (3), että kaikille $b \in K' - \{0_K\}$ pätee $1_K = bb^{-1} \in K'$, joten $b^{-1} = 1b^{-1} \in K'$. Siis ominaisuuden (3) nojalla $ab = a(b^{-1})^{-1} \in L'$ kaikilla $a \in K'$ ja $b \in K' - \{0_K\}$. Edellä näimme, että $0_K, 1_K \in K'$, joten ominaisuuden (2) nojalla $-1'_K$. Alirengastestin 3.17 nojalla siis K' on renkaan K alirengas.

Alirengas K' on kommutatiivinen koska K on kommutatiivinen. Lisäksi edellä näimme, että $b^{-1} \in K'$ kaikilla $b \neq 0_K$. Siis K' on kunta. \square

Kuntaominaisuudet säilyvät homomorfismeissa:

Propositio 4.8. *Olkoon K kunta ja olkoon R rengas, jossa on ainakin kaksi alkioita. Olkoon $\phi: K \rightarrow R$ rengashomomorfismi. Tällöin ϕ on injektio ja $\phi(K)$ on kunta.*

Todistus. Seurauksen 3.27 mukaan $\phi(K)$ on rengas, joka on Proposition 1.10 mukaan kommutatiivinen. Koska ϕ on rengashomomorfismi ja renkaassa R on vähintään kaksi alkioita, pätee Proposition 3.12 mukaan

$$\phi(0_K) = 0_R \neq 1_R = \phi(1_K).$$

Siis renkaassa $\phi(K)$ on vähintään kaksi alkioita. Yksikön kuva on yksikkö: Jos $u \in K^\times$, niin

$$\phi(u)\phi(u^{-1}) = \phi(uu^{-1}) = \phi(1_K) = 1_R.$$

Siis renkaan $\phi(K)$ nollasta poikkeavat alkiot ovat yksiköitä, joten $\phi(K)$ on kunta.

Olkoon $a \in \ker \phi$. Jos $a \neq 0$, niin

$$1 = \phi(1) = \phi(aa^{-1}) = 0\phi(a^{-1}) = 0,$$

mikä on mahdotonta. Siis ϕ on injektio Proposition 3.23 nojalla. \square

Jokaisella positiivisella reaaliluvulla $x > 0$ on positiivinen neliöjuuri $\sqrt{x} > 0$, jolle pätee $(\sqrt{x})^2 = x$. Negatiivisella reaaliluvulla ei ole reaalista neliöjuurta. Sen sijaan $(i\sqrt{-x})^2 = x$, joten kompleksilukuna ajateltuna luvulla $x < 0$ on neliöjuuri $i\sqrt{|x|}$, jolle käytämme merkintää \sqrt{x} .

Esimerkki 4.9. Olkoon $d \in \mathbb{Z} - \{0\}$ kokonaisluku, joka ei ole neliö. Olkoot

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \subset \mathbb{R},$$

kun $d \in \mathbb{N}$ ja

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \subset \mathbb{C},$$

kun $d \notin \mathbb{N}$. On helppo osoittaa, että $\mathbb{Q}(\sqrt{d})$ on rationaalilukujen kunnan laajennus, $\mathbb{Q}(\sqrt{d})$ on kunnan \mathbb{R} alikunta ja $\mathbb{Q}(i\sqrt{d})$ on kompleksilukujen kunnan alikunta, kun $d \in \mathbb{N} - \{0\}$. Samaan tapaan on helppo tarkastaa, että

$$\mathbb{Z}[d] = \{a + b\sqrt{d} \in \mathbb{C} : a, b \in \mathbb{Z}\}$$

on renkaan $\mathbb{Q}(\sqrt{d})$ alirengas.

Kunta $\mathbb{Q}(\sqrt{d})$ on kunnan \mathbb{Q} toisen asteen kuntalaajennus eli toisen asteen lukukunta. Kunta

$$\mathbb{Q}(i) = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Q}\}.$$

on Gaussin rationaalilukujen kunta. Kokonaisalueen

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}.$$

alkiot ovat Gaussin kokonaislukuja.

Esimerkki 4.10. Jos $a, b \in \mathbb{Z}$ ja $d \in \mathbb{Z} - \mathbb{N}$, niin $\mathbf{n}(a + b\sqrt{d}) = a^2 - b^2d \in \mathbb{N}$. Esimerkiksi renkaassa $\mathbb{Z}[\sqrt{-3}]$ $\mathbf{n}(\pm 1) = 1$, $\mathbf{n}(\pm i\sqrt{3}) = 3$, $\mathbf{n}(2) = 4 = \mathbf{n}(\pm 1 \pm i\sqrt{3})$ mutta minkään alkion normi ei ole 2 eikä 5.

4.3 Hamiltonin kvaterniot

Hamiltonin kvaterniot on joukko

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\} \subset M_2(\mathbb{C})$$

varustettuna renkaasta $M_2(\mathbb{C})$ indusoiduilla laskutoimituksilla.

Propositio 4.11. Hamiltonin kvaterniot on vino kunta.

Todistus. Proposition 3.17 avulla on helppo osoittaa, että \mathbb{H} on renkaan $M_2(\mathbb{C})$ alirengas. Lisäksi

$$\det \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = |a|^2 + |b|^2,$$

joten jokainen $A \in \mathbb{H} - \{0\}$ on kääntyvä matriisi. Itse asiassa kaikki nolasta poikkeavat alkiot ovat yksiköitä, koska

$$\frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \in \mathbb{H}$$

ja pätee

$$\frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = I_2.$$

Siis \mathbb{H} on jakorengas.

Jakorengas \mathbb{H} ei ole kommutatiivinen sillä esimerkiksi

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = - \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}. \quad \square$$

Kvaternioita käsitellessä on tapana käyttää esimerkiksi merkintöjä

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Tällöin

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \quad (4.1)$$

ja

$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}. \quad (4.2)$$

Matriisit 1 , \mathbf{i} , \mathbf{j} ja \mathbf{k} virittävät avaruuden \mathbb{H} neliulotteisena reaalisena vektoriavaruuksena, joten Hamiltonin kvaterniot voidaan esittää reaalisisina lineaarikombinaatioina

$$x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k},$$

$x_0, x_1, x_2, x_3 \in \mathbb{R}$, joilla voi laskea kuten kompleksiluvuilla huomioiden laskusäännöt (4.1) ja (4.2).

Esimerkki 4.12. Injektiivinen kuvaus $\phi: \mathbb{C} \rightarrow \mathbb{H}$, $\phi(z) = \text{diag}(z, \bar{z})$ on rengashomomorfismi, joten voimme samastaa sen kuvajoukon

$$\phi(\mathbb{C}) = \left\{ \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix} : z \in \mathbb{C} \right\} \subset M_2(\mathbb{C})$$

kompleksilukujen kunnan kanssa.

4.4 Lineaarialgebraa

Lineaarialgebran kursseilla käsitelty reaalisten vektoriavaruuksien ja lineaarikuvausten teoria yleistyy K -kertoimiseen tilanteeseen. Tässä luvussa tutustumme muutamaan määritelmään yleisessä tilanteessa ja näemme ensimmäiset sovellukset kuntien teoriaan. Lineaarialgebran perustulosten todistukset ovat samat kuin lineaarialgebran kursseilla, joten ohitamme niiden yksityiskohdat. Yleiseen kuntakertoimiseen lineaarialgebraan voi perehtyä monien lineaarialgebran ja algebran kirjojen avulla, esimerkiksi [Gre], [DF], [War].

Olkoon K kunta ja olkoon $(V, +)$ on kommutatiivinen ryhmä. **Vakiolla kertominen** on kuvaus $K \times V \rightarrow V$, $(\lambda, v) \mapsto \lambda v$, joka toteuttaa ehdot

- (1) $\lambda(v + w) = \lambda v + \lambda w$ kaikille $\lambda \in K$ ja $v, w \in V$,
- (2) $(\lambda + \mu)v = \lambda v + \mu v$ kaikille $\lambda, \mu \in K$ ja $v \in V$,
- (3) $\mu(\lambda v) = (\mu\lambda)v$ kaikille $\lambda, \mu \in K$ ja $v \in V$ ja
- (4) $1v = v$ kaikille $v \in V$.

Ryhmä V varustettuna tällä rakenteella on **K -vektoriavaruus**.

Propositio 4.13. *Olkoon K kunnan L alikunta. Tällöin L on K -vektoriavaruus.*

Todistus. Koska L on kunta, $(L, +)$ on kommutatiivinen ryhmä. Määritellään vakiolla kertominen $K \times L \rightarrow L$ asettamalla $(\lambda, v) \mapsto \lambda v$ kunnan L kertolaskuna. Tämä toimii, koska K on kunnan L alikunta. Ehdot (1)–(3) seuraavat kunnan L laskutoimitusten distributiivisuudesta ja assosiativisuudesta ja (4) seuraa siitä, että $1_K = 1_L$. \square

Esimerkki 4.14. Propositioiden 4.8 ja 4.4 nojalla kompleksilukujen kunnalla \mathbb{C} on alikunta $j(\mathbb{R})$, joka on isomorfinen reaalilukujen kunnan kanssa. Proposition 4.13 mukaan \mathbb{C} on \mathbb{R} -vektoriavaruus, kun määritellään vakiolla kertominen asettamalla $xz = j(x)z$ kaikilla $x \in \mathbb{R}$ ja $z \in \mathbb{C}$. Yleensä tällaisessa tilanteessa unohdetaan kuntahomomorfismi j ja ajatellaan, että $\mathbb{R} \subset \mathbb{C}$.

Lineaarisen riippuvuuden ja kannan määritelmät yleistävät suoraan vektoriavaruudessa \mathbb{R}^n lineaarialgebran kursseilla tavatut määritelmät.

Olkkoon K kunta ja olkkoon V K -vektoriavaruus. Joukko $A \subset V$ on **lineaarisesti riippumaton**, jos kaikille äärellisille joukoille $\{v_1, v_2, \dots, v_N\}$ ainoat kertoimet $a_1, a_2, \dots, a_N \in K$, joille pätee $\sum_{k=1}^N a_k v_k = 0$, ovat $a_1 = a_2 = \dots = a_N = 0$.

Vektorit $v_1, v_2, \dots, v_N \in V$ muodostavat K -vektoriavaruuden V **kannan**, jos jokaiselle $x \in V$ on yksikäsitteiset $x_1, x_2, \dots, x_N \in K$, joille pätee

$$x = \sum_{i=1}^N x_i v_i.$$

Lemma 4.15. Olkkoot $v_1, v_2, \dots, v_N \in V$ ja $w_1, w_2, \dots, w_M \in V$ K -vektoriavaruuden V kantoja. Tällöin $M = N$.

Todistus. Todistetaan kuten lineaarialgebran kurssilla. □

Olkkoon V K -vektoriavaruus, jolla on kanta, jossa on d alkioita. Tällöin avaruus V on **d -ulotteinen** ja sen **dimensio** on d .

Lemma 4.16. Olkkoon K kunta, jossa on N alkioita. Jos V on d -ulotteinen K -vektoriavaruus, niin avaruudessa V on N^d alkioita.

Todistus. Harjoitustehtävä. □

Esimerkki 4.17. Esimerkin 4.6 kunta F on 2-ulotteinen $\mathbb{Z}/2\mathbb{Z}$ -vektoriavaruus. Joukko $\{1, \alpha\}$ on sen kanta: Kannassa on oltava 2 alkioita Lemman 4.16 nojalla. Alkioille 1 ja α pätee $1 \neq 0$, $\alpha \neq 0$, $\alpha + 1 = \beta \neq 0$ kunnan F yhteenlaskutaulun mukaan.

Harjoitustehtäviä

- 4.1. Olkkoon $R \neq \{0\}$ rengas. Osoita, että yhteenlaskun neutraalialkio 0 ei ole yksikkö.
- 4.2. Osoita, että ei ole kuntahomomorfismia $\phi: \mathbb{R} \rightarrow \mathbb{Q}$.
- 4.3. Olkkoon K kunta ja olkkoon $K' \subset K$ vakaa osajoukko, joka on kunta indusoiduilla laskutoimituksilla. Osoita, että $0_{K'} = 0_K$ ja $1_{K'} = 1_K$.
- 4.4. Osoita, että ei ole kuntahomomorfismia $\phi: \mathbb{C} \rightarrow \mathbb{R}$.¹
- 4.5. Osoita, että $\mathbb{Q}(i)$ on kompleksilukujen kunnan alikunta.

¹Minne imaginaariyksikkö kuvautuisi?

4.6. Olkoon $d \in \mathbb{N} - \{0, 1\}$ luonnollinen luku, joka ei ole neliö. Osoita, että $\mathbb{Q}(\sqrt{d})$ on reaalilukujen kunnan alikunta.

4.7. Määritä Gaussin kokonaislukujen yksiköiden ryhmä. ²

4.8. Olkoon $d \in \mathbb{Z} - \{0\}$ kokonaisluku, joka ei ole neliö. Osoita, että

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \in \mathbb{R} : a, b \in \mathbb{Z}\},$$

on reaalilukujen renkaan alirengas.

4.9. Osoita, että $\mathbb{Z}[\sqrt{2}]^\times$ on ääretön. ³

4.10. Osoita, että Hamiltonin kvaterniot muodostavat renkaan.

4.11. Osoita, että yhtälöllä $x^2 = -1$ on äärettömän monta ratkaisua Hamiltonin kvaternioiden vinossa kunnassa. ⁴

4.12. Todista Lemma 4.16.

²Käytä kompleksilukujen normin tai modulin ominaisuuksia.

³Etsi sopiva yksikkö ja käytä Propositiota 4.1

⁴Tarkastele kvaternioita, jotka ovat muotoa $a\mathbf{i} + b\mathbf{j} + c\mathbf{k}$, $a^2 + b^2 + c^2 = 1$.

Luku 5

Jaollisuus

5.1 Jaollisuudesta

Jaollisuus määritellään kommutatiivisessa renkaassa samalla tavalla kuin kokonaislukujen tapauksessa:

Jos K on kommutatiivinen rengas ja $a, b, c \in K$ siten, että $ab = c$, niin a ja b ovat alkion c tekijöitä. Tällöin alkiot a ja b jakavat alkion c , mistä käytetään merkintää $a \mid c$ ja vastaavasti $b \mid c$.

Seuraavat jaollisuuden perusominaisuudet on helppo tarkastaa kuten kokonaislukujen tapauksessa.

Propositio 5.1. *Olkoon K kommutatiivinen rengas. Tällöin*

- (1) $a \mid a$ kaikille $a \in K$.
- (2) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.
- (3) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

Todistus. Harjoitustehtävä 5.1. □

Olkoon R rengas, jossa on vähintään 2 alkioita. Jos $a, b \in R$, $a, b \neq 0$ ja $ab = 0$, niin a ja b ovat nollan jakajia.

Kommutatiivinen rengas R , jossa ei ole nollan jakajia, on kokonaisalue.

Esimerkki 5.2. (a) Kokonaislukujen rengas on kokonaisalue.

(b) Olkoon $n \geq 2$ ja olkoon R rengas. Jos $A, B \in M_n(R)$ ovat neliömatriiseja, joiden ainoat nollasta poikkeavat kertoimet ovat A_{11} ja B_{nn} , niin $AB = 0$. Siis matriisit A ja B ovat nollan jakajia.

(c) Jos $q = cd$ joillain $c, d \in \mathbb{N} - \{0, 1\}$, niin $c + q\mathbb{Z} \neq 0 \in \mathbb{Z}/q\mathbb{Z}$, $d + q\mathbb{Z} \neq 0 \in \mathbb{Z}/q\mathbb{Z}$ ja $(c + q\mathbb{Z})(d + q\mathbb{Z}) = 0 \in \mathbb{Z}/q\mathbb{Z}$, joten $\mathbb{Z}/q\mathbb{Z}$ ei ole kokonaisalue.

Esimerkki 5.3. Esimerkki 5.2(c) osoittaa, että kokonaisalueen kuva rengashomomorfismissa ei välttämättä ole kokonaisalue.

Propositio 5.4. *Yksikkö ei ole nollan jakaja.*

Todistus. Olkoon a yksikkö ja oletetaan, että $ab = 0$. Silloin $b = a^{-1}0 = 0$. Vastaavasti nähdään, että $b = 0$, jos $ba = 0$. \square

Seuraus 5.5. *Jakorengaassa ei ole nollan jakajia. Erityisesti kunta on kokonaisalue.* \square

Renkaassa R pätee **kertolaskun supistussääntö**, jos $b = c$ aina, kun jollekin $a \in R - \{0\}$ pätee $ab = ac$ tai $ba = ca$.

Renkaan kertolaskun supistussääntö poikkeaa hieman Luvussa 3.2 tarkastellusta laskutoimituksen supistussäännöstä, koska $0a = 0$ kaikille $a \in R$.

Propositio 5.6. *Kommutatiivinen rengas K on kokonaisalue, jos ja vain jos kertolaskun supistussääntö pätee renkaassa K .*

Todistus. Harjoitustehtävä 5.2 \square

Propositio 5.7. *Kokonaisalueen karakteristika on 0 tai alkuluku.*

Todistus. Olkoon R rengas, jonka karakteristika on $\chi(R) = ab$, missä $a, b \notin \{0, 1\}$. Proposition 3.28 nojalla on täsmälleen yksi rengashomomorfismi $\phi: \mathbb{Z} \rightarrow R$. Karakteristikan määritelmän mukaan $\phi(ab) = 0$. Nyt $\phi(a), \phi(b) \neq 0$, koska $1 < a, b < ab$, ja $\phi(a)\phi(b) = \phi(ab) = 0$, joten R ei ole kokonaisalue. \square

Lause 5.8. *Äärellinen kokonaisalue on kunta.*

Todistus. Olkoon E kokonaisalue ja olkoon $a \in E - \{0\}$. Kuvaus $\ell_a: E \rightarrow E$, $\ell_a(x) = ax$ on injektio Proposition 5.6 nojalla. Kun oletamme lisäksi, että E on äärellinen, niin kuvaus ℓ_a on myös surjektio. Tällöin on $\bar{a} \in E$, jolle $a\bar{a} = \ell_a(\bar{a}) = 1$. Koska E on kommutatiivinen, $\bar{a} = a^{-1}$. \square

Seuraava samanhenkinen tulos on vaikeampi todistaa:

Lause 5.9 (Wedderburnin lause). *Äärellinen jakorengas on kunta.*

Todistus. Katso esimerkiksi [War, Theorem 39.9]. \square

Proposition 5.8 avulla saamme tärkeän tuloksen äärellisen kunnan koosta:

Lause 5.10. *Äärellisessä kunnassa on p^q alkia jollakin alkuluvulla p ja jollakin $q \in \mathbb{N} - \{0\}$.*

Todistus. Olkoon K äärellinen kunta. Tällöin kunnan K karakteristika on Proposition 5.7 nojalla p jollain alkuluvulla p . Olkoon $\phi: \mathbb{Z} \rightarrow K$ rengashomomorfismi. Karakteristikan määritelmän ja Proposition 5.8 nojalla alirengas $k = \phi(\mathbb{Z}) \subset K$ on p alkioista koostuva alikunta. Koska Proposition 4.13 nojalla K on k -vektoriavaruus, niin väite seuraa Lemmasta 4.16. \square

5.2 Jaottomat alkiot ja alkualkiot

Kokonaisalueen E alkio $p \in E - (E^\times \cup \{0\})$ on **jaoton**, jos a tai b on yksikkö aina, kun $p = ab$.

Kokonaisalueen K alkio $p \in K - (K^\times \cup \{0\})$ on **alkualkio** (tai **alkuluku**), jos kaikille $a, b \in K$ pätee $p \mid a$ tai $p \mid b$, jos $p \mid ab$.^a

^aEsimerkiksi kokonaislukuja käsiteltäessä merkintä p varataan usein alkualkioille tai alkuluville. Tämä johtuu siitä, että alkuluku on englanniksi prime, saksaksi Primzahl, ranskaksi nombre premier.

Propositio 5.11. *Kokonaisalueen alkualkiot ovat jaottomia.*

Todistus. Olkoon K kokonaisalue ja olkoon $p \in K$ alkualkio. Oletetaan, että $p = ab$. Riittää tarkastella tapaus $p \mid a$. Tällöin $a = pc$ jollakin $c \in K$, joten $p = pcb$. Proposition 5.6 nojalla kertolaskun supistussääntö on voimassa kokonaisalueessa K , joten b on yksikkö. Siis p on jaoton. \square

Propositio 5.12 (Eukleideen lemma). *Kokonaislukujen renkaan jaottomat alkiot ovat alkualkioita.*

Todistus. Katso Propositio A.6. \square

Kokonaislukujen renkaassa jaottomat alkiot ja alkualkiot ovat samoja Eukleideen lemmän ja Proposition 5.11 nojalla. Näillä määritelmillä luvut $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29$ ja niin edelleen ovat renkaan \mathbb{Z} alkualkioita ja jaottomia alkioita.

Kokonaislukujen yhteydessä käsitellään yleensä **alkulukuja**, jotka ovat kokonaislukujen renkaan positiiviset alkualkiot.

Kokonaislukuja yleisemmissä kokonaisalueissa jaottomat alkiot eivät kaikissa tapauksissa välttämättä ole alkualkioita.

Lemma 5.13. *Olkoon d negatiivinen kokonaisluku. Jos $a \mid b$ renkaassa $\mathbb{Z}[\sqrt{d}]$, niin $\bar{a} \mid \bar{b}$ renkaassa $\mathbb{Z}[\sqrt{d}]$ ja $\mathbf{n}(a) \mid \mathbf{n}(b)$ renkaassa \mathbb{Z} .*

Todistus. Jos $b = ac$, niin Proposition 1.22 nojalla $\bar{b} = \overline{ac} = \bar{a}\bar{c}$, joten $\bar{a} \mid \bar{b}$. Jos $c = c_1 + ic_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, niin $\mathbf{n}(c) = c\bar{c} = c_1^2 + dc_2^2 \in \mathbb{Z}$. Lisäksi $\mathbf{n}(b) = \mathbf{n}(ac) = \mathbf{n}(a)\mathbf{n}(c)$, joten $\mathbf{n}(a) \mid \mathbf{n}(b)$. \square

Esimerkki 5.14. (1) Renkaassa $\mathbb{Z}[\sqrt{-3}]$ pätee

$$4 = 2^2 = \mathbf{n}(2) = \mathbf{n}(1 \pm i\sqrt{3}) = (1 + i\sqrt{3})(1 - i\sqrt{3}).$$

Koska renkaassa $\mathbb{Z}[\sqrt{-3}]$ ei ole alkioita, joiden normi on 2, nähdään Lemman 5.13 nojalla, että alkiot 2 ja $1 \pm i\sqrt{3}$ ovat kaikki jaottomia. Nyt $2 \mid 4$ mutta $2 \nmid 1 \pm i\sqrt{3}$, sillä renkaan $\mathbb{Z}[\sqrt{-3}]$ ainoat alkiot, joiden normi on 1 ovat 1 ja -1 , jotka ovat yksiköitä. Siis 2 ei ole alkualkio.

(2) Renkaassa $\mathbb{Z}[\sqrt{10}]$ voidaan osoittaa, että alkiot 2, 3, $4 + \sqrt{10}$ ja $4 - \sqrt{10}$ ovat jaottomia mutta eivät alkualkioita, koska

$$2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$$

mutta 2 tai 3 ei ole lukujen $(4 \pm \sqrt{10})$ tekijä ja vastaavasti $(4 \pm \sqrt{10})$ ei ole lukujen 2 tai 3 tekijä.

5.3 Renkaan $\mathbb{Z}/q\mathbb{Z}$ yksiköt

Sovellamme nyt liitteessä A kerrattavia kokonaislukujen jaollisuustuloksia jäännösluokkarenkaan $\mathbb{Z}/q\mathbb{Z}$ yksiköiden ryhmän ominaisuuksien tarkasteluun.

Propositio 5.15. *Olkoon $q \geq 2$. Tällöin $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on yksikkö, jos ja vain jos $\text{syt}(a, q) = 1$. Jos p on alkuluku ja $a \not\equiv 0 \pmod{p}$, niin $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$.*

Todistus. Jäännösluokka $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on yksikkö, jos ja vain jos on $b \in \mathbb{Z}$, jolle pätee

$$1 + q\mathbb{Z} = (a + q\mathbb{Z})(b + q\mathbb{Z}) = ab + q\mathbb{Z}.$$

Tämä on yhtäpitävää ehdon $ab \equiv 1 \pmod{q}$ kanssa, joka taas pätee, jos ja vain jos on $c \in \mathbb{Z}$, jolle $ab = 1 + cq$. Tämä Bézout'n yhtälön¹ nojalla yhtäpitävää sen kanssa, että $\text{syt}(a, q) = 1$. \square

Seuraus 5.16. *Jos p on alkuluku, niin $\mathbb{Z}/p\mathbb{Z}$ on kunta.*

Todistus. Jos p on alkuluku, niin $\text{syt}(a, p) = 1$ kaikille $a \in \{1, 2, \dots, p-1\}$, joten renkaan $\mathbb{Z}/p\mathbb{Z}$ kaikki nollasta poikkeavat alkiot ovat yksiköitä. \square

Propositio 5.17. *Olkoon $q \geq 2$. Alkio $a + q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z}) - \{0\}$ on nollan jakaja, jos ja vain jos $\text{syt}(a, q) > 1$. Jos q ei ole alkuluku, niin renkaassa $\mathbb{Z}/q\mathbb{Z}$ on nollan jakajia.*

Todistus. Väite seuraa Propositioista 5.15 ja 5.4 ja Esimerkin 5.2 kohdasta (3). \square

Seuraus 5.18. *Renkaan $\mathbb{Z}/q\mathbb{Z}$ nollasta poikkeava alkio on joko nollan jakaja tai yksikkö.*

Todistus. Seuraa Propositioista 5.17 ja 5.15. \square

Seuraava tulos on yhteenveto tuloksista, jotka koskevat jäännösluokkarenkaan $\mathbb{Z}/q\mathbb{Z}$ ominaisuuksien riippuvuutta luvusta q .

Lause 5.19. *Seuraavat väitteet ovat yhtäpitäviä:*

(1) $\mathbb{Z}/q\mathbb{Z}$ on kokonaisalue.

(2) $\mathbb{Z}/q\mathbb{Z}$ on kunta.

(3) q on alkuluku.

Todistus. Seuraa Propositioista 5.15 ja 5.17. \square

Kongruenssiluokkien renkaassa $\mathbb{Z}/q\mathbb{Z}$ jokainen nollasta poikkeava alkio on joko yksikkö tai nollan jakaja. Vastaava tulos ei päde renkaille yleisesti, sillä kokonaislukujen renkaassa ei ole nollan jakajia ja siinä on ainoastaan kaksi yksikköä ± 1 .

¹Propositio A.3

Harjoitustehtäviä

5.1. Olkoon K kommutatiivinen rengas. Osoita, että

- (1) $a \mid a$ kaikille $a \in K$.
- (2) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.
- (3) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

5.2. Todista Propositio 5.6.

5.3. (1) Olkoon K kommutatiivinen rengas. Olkoon $u \in K^\times$ ja olkoon $a \in K$. Osoita, että $a \in K^\times$, jos $a \mid u$.

(2) Olkoon K kokonaisalue. Jos $a \mid b$ ja $b \mid a$, niin $a = ub$ jollain $u \in K^\times$.

5.4. Olkoon D äärellinen rengas, jossa ei ole nollanjakajia. Osoita, että

- (1) jokaisella $d \in D - \{0\}$ on vasen ja oikea käänteisalkio kertolaskun suhteen, ja
- (2) D on jakorengas.²

5.5. Osoita, että $\mathbb{Z}[i]$ on kokonaisalue. Osoita, että $1 + i$ on jaoton renkaassa $\mathbb{Z}[i]$.

5.6. Olkoon p alkuluku ja olkoon

$$K = \left\{ \frac{r}{s} : r, s \in \mathbb{Z}, s \not\equiv 0 \pmod{p} \right\} \subset \mathbb{Q}.$$

(1) Osoita, että K on rationaalilukujen renkaan alirengas.

(2) Osoita, että $\frac{a}{b} \in K$ on yksikkö, jos ja vain jos a ei ole jaollinen alkuluvulla p .

(3) Missä kohtaa käytimme oletusta, että p on alkuluku?

5.7. Olkoot $q_1, q_2, \dots, q_N \in \mathbb{Z}$ siten, että $\text{sy}(q_i, q_j) = 1$ kaikilla $i \neq j$. Olkoon $k \in \mathbb{Z}$ siten, että $q_i \mid k$ kaikilla $1 \leq i \leq N$. Osoita, että $\prod_{i=1}^N q_i \mid k$.

5.8. Määritä renkaan $\mathbb{Z}/10\mathbb{Z}$ yksiköt ja nollan jakajat.

²Katso määritelmät luvusta 1.6. Lauseen 5.8 todistus antaa idean kohdan (1) todistukseen, kohdassa (2) pitää vielä näyttää, että vasen ja oikea käänteisalkio ovatkin sama alkio.

Luku 6

Polynomirenkaat

Tässä luvussa määrittelemme polynomit, joiden kertoimet ovat kommutatiivisessa renkaassa ja määrittelemme niille laskutoimitukset, jotka ovat samat kuin tutussa reaali kertomisessa tapauksessa. Näin saamme määriteltyä tärkeän luokan renkaita, yhden muuttujan polynomirenkaat, joita käytetään kurssin viimeisessä luvussa kuntalaaajennusten ja erityisesti äärellisten kuntien konstruktiossa.

6.1 Polynomit ja polynomifunktiot

Tässä luvussa ja myöhemmin polynomeja käsiteltäessä X on muodollinen symboli, jota usein kutsutaan muuttujaksi.

Olkoon K kommutatiivinen rengas. Olkoon $n \in \mathbb{N}$ ja olkoot $a_n, a_{n-1}, \dots, a_1, a_0 \in K$.
Lauseke

$$P(X) = \sum_{k=0}^n a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

on **yhden muuttujan K -kertoiminen polynomi**. Jos $m > n$ ja $a_{n+1} = a_{n+2} = \dots = a_m = 0$, niin

$$\sum_{k=0}^n a_k X^k = \sum_{k=0}^m a_k X^k.$$

Olkoon

$$K[X] = \left\{ \sum_{k=0}^n a_k X^k : n \in \mathbb{N}, a_k \in K \text{ kaikilla } 0 \leq k \leq n \right\}.$$

Olkoon K kommutatiivinen rengas. Polynomien $P(X) = \sum_{k=0}^n a_k X^k \in K[X]$ määräämä **polynomifunktio** on $P: K \rightarrow K$,

$$x \mapsto \sum_{k=0}^n a_k x^k = P(x).$$

Algebrassa tulee pitää erillään polynomien ja polynomifunktion käsitteet ja siksi on hyvä käyttää määritelmän polynomille ja polynomifunktiolle selkeästi erilaisia merkintätapoja.

Polynomirengas voi olla paljon suurempi joukko kuin vastaava polynomifunktioiden joukko: Jos K on kommutatiivinen rengas, jossa on ainakin kaksi alkia, niin polynomirengas $K[X]$ on ääretön. Kuitenkin, jos K on äärellinen, niin funktioita joukolta K joukkoon K on ainoastaan äärellinen määrä.

Kun tarkastelemme polynomirengasta $(\mathbb{Z}/q\mathbb{Z})[X]$, merkitsemme kerrointa $a + q\mathbb{Z}$ yksinkertaisuuden vuoksi edustajalla a .

Esimerkki 6.1. Olkoot $Q(X) = X^2, P(X) = X \in (\mathbb{Z}/2\mathbb{Z})[X]$. Tällöin $Q(X) \neq P(X)$ mutta

$$P(0) = 0 = 0^2 = Q(0) \quad \text{ja} \quad P(1) = 1 = 1^2 = Q(1),$$

joten polynomit $P(X)$ ja $Q(X)$ määräävät saman funktion $P = Q: \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$. Nollasta poikkeava polynomi $Q(X) - P(X) = X^2 - X = X^2 + X$ määrää nollakuvauksen renkaalta $\mathbb{Z}/2\mathbb{Z}$ itselleen.

6.2 Polynomirengas

Tässä luvussa määrittelemme K -kertoimisten polynomien joukossa kaksi laskutoimitusta ja tarkastelemme näin saatavan renkaan perusominaisuuksia.

Olkoon K kommutatiivinen rengas. Polynomien

$$P(X) = \sum_{k=1}^n a_k X^k \in K[X] \quad \text{ja} \quad Q(X) = \sum_{k=1}^n b_k X^k \in K[X]$$

summa on

$$P(X) + Q(X) = \sum_{k=0}^n (a_k + b_k) X^k \in K[X] \tag{6.1}$$

ja niiden tulo on

$$P(X)Q(X) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) X^k \in K[X]. \tag{6.2}$$

Propositio 6.2. *Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkia. Joukko $K[X]$ varustettuna polynomien yhteen- ja kertolaskulla on kommutatiivinen rengas.*

Todistus. Selvästi polynomit 0 ja 1 ovat yhteenlaskun ja kertolaskun neutraali-alkiot. Muut renkaan määrittelevät ominaisuudet seuraavat suoraviivaisesti siitä, että K on kommutatiivinen rengas. □

Olkoon K kommutatiivinen rengas, jossa on ainakin 2 alkia. Rengas $K[X]$ on K -kertoiminen polynomirengas.

Polynomirenkaat ovat tärkeitä kommutatiivisia renkaita. Sovellamme niitä äärellisten esimerkiksi kuntien konstruktiossa.

Luku a_0 on polynomien $\sum_{k=1}^n a_k X^k$ vakiotermi.

Lemma 6.3. *Olko K kommutatiivinen rengas. Kuvaus $i: K \rightarrow K[X]$, joka kuvaa renkaan K alkion a polynomiksi $a = aX^0 \in K[X]$, on injektiiivinen rengashomomorfismi.*

Todistus. Kuvaus i kuvaa ainoastaan alkion $0 \in K$ nollapolynomiksi, joten Proposition 3.23 nojalla i on injektio, kunhan se osoitetaan homomorfismiksi. Olkoot siis $a, b \in K$. Tällöin polynomien laskutoimituksen määritelmän nojalla

$$i(a) + i(b) = aX^0 + bX^0 = (a + b)X^0 = i(a + b)$$

ja

$$i(a) i(b) = aX^0 bX^0 = abX^0 = i(ab).$$

Lisäksi $i(1) = 1 \cdot X^0$, joten i on homomorfismi. □

Propositio 6.4. *Olko K kommutatiivinen rengas. Olko $F: K[X] \rightarrow \mathcal{F}(K, K)$ kuvaus, $F(P(X)) = P$. Tällöin F on rengashomomorfismi.*

Todistus. Harjoitustehtävä 6.6. □

Kommutatiivinen rengas K on polynomien $P(X) \in K[X]$ kerroinrengas.

Propositio 6.5. *Polynomirenkaan karakteristika on sama kuin sen kerroinrenkaan karakteristika.*

Todistus. Lemman 6.3 mukaan polynomirenkaalla $K[X]$ on kerroinrenkaan K kanssa isomorfinen alirengas $S = \{aX^0 : a \in K\}$. Renkaan $K[X]$ kertolaskun neutraalialkio on renkaassa S , joten renkailla $K[X]$ ja S on sama karakteristika. □

6.3 Polynomien vaihtoehtoinen määritelmä

Huomaa, että polynomeille $P(X), Q(X) \in K[X]$ pätee $P(X) = Q(X)$ täsmälleen silloin, kun niiden kerroinjonot ovat samat. Vähemmän havainnollinen mutta edellä esitettyä täsmällisempi ja sen kanssa yhtäpitävä tapa määritellä polynomit on korvata polynomien lauseke $\sum_{k=0}^n a_k X^k$ sen kertoimien muodostamalla jonolla $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ ja määritellä yhteenlasku komponenteittain kuten jonoille on tapana ja kertolasku kaavan (6.2) mukaisesti. Tällöin jono $(0, 1, 0, 0, 0, \dots)$ on symbolin X vastine. Seuraavassa määritelmässä jono $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ ajatellaan funktiona $\omega: \mathbb{N} \rightarrow K$ siten, että $\omega(k) = a_k$ kaikilla $k \in \mathbb{N}$.

Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkioita. Kuvaus $\omega: \mathbb{N} \rightarrow K$, jolle on $N_\omega \in \mathbb{N}$ siten, että $\omega(k) = 0$ kaikille $k \geq N_\omega$, on K -kertoiminen polynomi.

Joukko

$$K[X] = \{\omega: \mathbb{N} \rightarrow K\}$$

varustettuna laskutoimituksilla

$$(\omega + \omega')(k) = \omega(k) + \omega'(k)$$

ja

$$(\omega\omega')(k) = \sum_{i,j \in \mathbb{N}: i+j=k} \omega(i)\omega'(j)$$

on K -kertoiminen polynomirengas.

6.4 Aste

Olkoot $a_n, a_{n-1}, \dots, a_1, a_0 \in K$ ja olkoon $a_n \neq 0$. Polynomin

$$P(X) = \sum_{k=0}^n a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

aste on $\deg(P(X)) = n$ ja a_n on polynomin $P(X)$ korkeimman asteen kerroin.

Nollapolynomin 0 aste on $-\infty$.

Symbolilla $-\infty$ on seuraavat ominaisuudet:

- $-\infty < a$ kaikilla kokonaisluvuilla a ,
- $-\infty + -\infty = -\infty$ ja
- $-\infty + a = -\infty$ kaikilla kokonaisluvuilla a .

Symbolille $-\infty$ ei ole määritelty muita operaatioita, käytämme sitä ainoastaan nollapolynomin asteen merkinä.

Esimerkki 6.6. (1) Olkoot $P(X), Q(X) \in \mathbb{Z}[X]$,

$$P(X) = 2X^2 + 2, \quad Q(X) = 1 + 2X.$$

Tällöin

$$P(X)Q(X) = 4X^3 + 2X^2 + 4X + 2.$$

Nyt $\deg(P(X)) = 2$, $\deg(Q(X)) = 1$ ja $\deg(P(X)Q(X)) = 3$.

(2) Jos polynomit $P(X), Q(X) \in (\mathbb{Z}/4\mathbb{Z})[X]$ määritellään samoilla lausekkeilla kuinkohdassa (1), niin

$$P(X)Q(X) = 2X^2 + 2.$$

Nyt pätee $P(X)Q(X) = P(X) = P(X) \cdot 1$ mutta $Q(X) \neq 1$, joten kertolaskun supistus sääntö ei päde polynomirengas $(\mathbb{Z}/4\mathbb{Z})[X]$.

Lisäksi pätee $\deg(P(X)) = 2$ ja $\deg(Q(X)) = 1$ mutta

$$\deg(P(X)Q(X)) = 2 < 3 = 2 + 1$$

ja

$$-\infty = \deg 0 = \deg((2X)(2X)) < 2 \deg(2X) = 2.$$

Lemma 6.7. *Olkoon K kommutatiivinen rengas, $K \neq \{0\}$. Tällöin*

$$\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X)$$

kaikille $P(X), Q(X) \in K[X]$.

Todistus. Olkoot $P(X) = \sum_{k=0}^n a_k X^k$ ja $Q(X) = \sum_{k=0}^m b_k X^k$ ja oletetaan, että $a_n \neq 0$, $b_m \neq 0$. Tulopolynomin $P(X)Q(X)$ korkeimman asteen termi on $a_n b_m X^{n+m}$, jos $a_n b_m \neq 0$, muuten aste on alempi. \square

Seuraava tulos osoittaa, että kokonaisalueominaisuus periytyy kerroinrenkaasta polynomirenkaaseen.

Propositio 6.8. *Jos K on kokonaisalue ja $P(X), Q(X) \in K[X]$, niin*

$$\deg(P(X)Q(X)) = \deg(P(X)) + \deg(Q(X)).$$

Lisäksi $K[X]$ on kokonaisalue.

Todistus. Lemman 6.7 merkinnöillä tulopolynomin korkeimman asteen termin kerroin on $a_n b_m \neq 0$, sillä K on kokonaisalue. Erityisesti kahden nollassa poikkeavan polynomin tulo ei ole nollapolynomi, koska tulon aste on luonnollinen luku. \square

Seuraus 6.9. *Olkoon $K \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$. Tällöin*

$$\deg(P(X)Q(X)) = \deg P(X) + \deg Q(X)$$

kaikille $P(X), Q(X) \in K[X]$. \square

Propositio 6.10. *Jos K on kunta, niin $P(X) \in K[X]^\times$, jos ja vain jos $\deg P(X) = 0$.*

Todistus. Jos $Q(X) \in K[X] - \{0\}$, niin

$$\deg(P(X)Q(X)) = \deg P(X) + \deg Q(X) \geq \deg P(X),$$

joten $P(X)$ ei ole yksikkö, jos $\deg P(X) \geq 1$. Jos taas $\deg P(X) = 0$, niin $P(X) = aX^0$ jollain $a \in K^\times$ ja pätee $aX^0 a^{-1}X^0 = 1X^0$, joten aX^0 on yksikkö. \square

Polynomirengas ei ole koskaan kunta. Jos K on kokonaisalue, niin Proposition 6.8 mukaan ainoat polynomit, joilla on käänteisalkio kertolaskun suhteen, ovat vakiopolynomit u , missä $u \in K^\times$. Sen sijaan, jos kerroinrengas ei ole kokonaisalue, niin esimerkiksi vakio-
polynomeilla a , missä a on nollan jakaja renkaassa K , ei ole käänteisalkiota Propositioiden 5.4 ja 6.2 nojalla.

Propositioista 6.8 seuraa, että ensimmäisen asteen polynomit ovat jaottomia kuntakertoimisessa polynomirenkaassa, koska kaikki nollassa poikkeavat polynomit, joiden aste on pienempi kuin 1 ovat vakiopolynomeita, siis yksiköitä. Korkeamman asteen polynomin osoittaminen jaottomaksi ei ole välttämättä kovin helppoa.

6.5 Polynomien jakoyhtälö

Yleistämme nyt kokonaislukujen jakoyhtälön¹ polynomirengasille.

Lause 6.11 (Jakoyhtälö). *Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkioita. Olkoot $A(X), B(X) \in K[X]$ siten, että $B(X) \neq 0$ ja polynomin $B(X)$ korkeimman asteen termin kerroin on yksikkö. Tällöin on yksikäsitteiset polynomit $Q(X), J(X) \in K[X]$, joille pätee*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$.

Todistus. Osoitetaan ensin, että on polynomit $Q(X)$ ja $J(X)$, jotka toteuttavat väitteen yhtälön. Jos $B(X)$ jakaa polynomin $A(X)$, ei ole mitään todistettavaa. Muuten olkoon

$$S = \{A(X) - D(X)B(X) : D(X) \in K[X]\}.$$

Koska $B(X)$ ei jaa polynomia $A(X)$, niin $0 \notin S$, joten joukko

$$\deg S = \{\deg P(X) : P(X) \in S\}$$

on luonnollisten lukujen joukon epätyhjä osajoukko ja sillä on siis minimi $m \geq 0$.

Olkoon $Q(X) \in K[X]$ polynomi, jolle pätee $\deg(A(X) - Q(X)B(X)) = m$. Olkoon

$$J(X) = A(X) - Q(X)B(X) = a_m X^m + \cdots + a_0.$$

Nyt polynomit $Q(X)$ ja $J(X)$ siis toteuttavat väitteen yhtälön.

Osoitetaan sitten, että $m < d = \deg B(X)$. Olkoon b_d polynomin $B(X)$ korkeimman asteen kerroin, joka on oletuksen mukaan yksikkö. Jos olisi $m \geq d$, niin

$$J(X) - a_m b_d^{-1} X^{m-d} B(X) = A(X) - (Q(X) + a_m b_d^{-1} X^{m-d}) B(X) \in S$$

ja $\deg(J(X) - a_m b_d^{-1} X^{m-d} B(X)) < m$, mutta tämä on mahdotonta, koska polynomin $J(X)$ aste on minimaalinen.

Osoitetaan lopuksi polynomien $Q(X)$ ja $J(X)$ yksikäsitteisyys. Jos $\tilde{Q}(X)$ ja $\tilde{J}(X)$ ovat polynomeja, joille pätee

$$A(X) = \tilde{Q}(X)B(X) + \tilde{J}(X)$$

ja $\deg \tilde{J}(X) < d$, niin

$$(Q(X) - \tilde{Q}(X))B(X) = \tilde{J}(X) - J(X).$$

Jos $\tilde{Q}(X) \neq Q(X)$, niin yhtälön vasemman puolen polynomin aste on vähintään d . Kuitenkin, koska $\deg J(X) < d$ ja $\deg \tilde{J}(X) < d$, niin

$$\deg(\tilde{J}(X) - J(X)) < d.$$

Siis $\tilde{Q}(X) = Q(X)$ ja $\tilde{J}(X) = J(X)$. □

¹Propositio A.1

Seuraus 6.12 (Kuntakertoimisten polynomien jakoyhtälö). *Olkoon K kunta. Olkoot $A(X)$, $B(X) \in K[X]$ siten, että $B(X) \neq 0$. Tällöin on yksikäsitteiset $Q(X), J(X) \in K[X]$, joille*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$. □

Esimerkki 6.13. Jakoyhtälö voidaan toteuttaa algoritmisesti jakokulman avulla kuten kokonaisluvuillekin. Tällöin jakokulma antaa esimerkiksi polynomeille

$$A(X) = 2X^3 + X^2 - X - 1 \quad \text{ja} \quad B(X) = X^2 - 2$$

renkaassa $\mathbb{Z}[X]$

$$\begin{array}{r} X^2 - 2 \overline{) \begin{array}{r} 2X^3 + X^2 - X - 1 \\ \underline{\mp 2X^3} \\ X^2 + 3X - 1 \\ \underline{ 2X} \\ X^2 \underline{ 2} \\ \phantom{\underline{ 2}} \\ 3X + 1 \end{array} \end{array}$$

Toisin sanoen

$$2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 3X + 1,$$

joten Jakoyhtälön merkinnöillä $Q(X) = 2X + 1$ ja $J(X) = 3X + 1$.

Esimerkki 6.14. Olkoot $A(X), B(X) \in (\mathbb{Z}/3\mathbb{Z})[X]$ polynomit, joilla on sama lauseke kuin Esimerkissä 6.13. Tällöin pätee

$$2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 1 = (2X + 1)(X^2 + 1) + 1. \quad (6.3)$$

Jos $B(X) = 2X + 1$, niin jakoyhtälö ei toimi renkaassa $\mathbb{Z}[X]$, koska polynomin $B(X)$ korkeimman asteen kerroin ei ole yksikkö. Tällöin jakokulmassa päädytään ongelmalliseen tilanteeseen

$$2X^3 + X^2 - X - 1 = X^2(2X + 1) - X - 1,$$

josta ei voi jatkaa. Sen sijaan renkaassa $(\mathbb{Z}/3\mathbb{Z})[X]$ voidaan jatkaa, koska $\mathbb{Z}/3\mathbb{Z}$ on kunta. Nyt

$$-X - 1 = 2X + 2 = (2X + 1) + 1$$

ja päädytään yhtälöön (6.3). Renkaassa $\mathbb{Q}[X]$ jakoa voi myös jatkaa ja saadaan

$$2X^3 + X^2 - X - 1 = (X^2 - \frac{1}{2})(2X + 1) - \frac{1}{2}.$$

6.6 Polynomien juuret ja jaollisuus

Olkoon K kommutatiivinen rengas ja olkoon $P(X) \in K[X]$. Alkio $c \in K$ on polynomin $P(X)$ **juuri**, jos $P(c) = 0$.

Esimerkki 6.15. (1) Esimerkin 6.6(1) polynomeilla $P(X), Q(X) \in \mathbb{Z}[X]$ ei ole juuria. Sen sijaan samalla lausekkeella määritellyllä rationaalilukukertoimisella polynomilla $Q(X) \in \mathbb{Q}[X]$ on juuri: $Q(-\frac{1}{2}) = 0$.

(2) Esimerkin 6.6(2) polynomilla $P(X) \in (\mathbb{Z}/4\mathbb{Z})[X]$ on kaksi juurta: $P(1) = 2 \cdot 1^2 + 2 = 4 \equiv 0 \pmod{4}$ ja $P(3) = 2 \cdot 3^2 + 2 \equiv 0 \pmod{4}$. Sen sijaan on helppo tarkastaa, että polynomilla $Q(X) \in (\mathbb{Z}/4\mathbb{Z})[X]$ ei ole juuria.

(3) Esimerkin 6.1 polynomilla $X^2 + X = X(X + 1) \in (\mathbb{Z}/2\mathbb{Z})[X]$ on kaksi juurta.

Jakoyhtälö antaa seuraavan perustuloksen:

Propositio 6.16. *Olkoon K kommutatiivinen rengas, jossa on vähintään kaksi alkioita. Olkoon $P(X) \in K[X]$ ja $c \in K$. Tällöin c on polynomin P juuri, jos ja vain jos $(X - c) \mid P(X)$.*

Todistus. Oletetaan, että $P(c) = 0$. Koska polynomin $X - c$ korkeimman asteen termin kerroin on $1 \in K^\times$, voimme soveltaa jakoyhtälöä.² Jakoyhtälön mukaan on K -kertoimiset polynomit $Q(X)$ ja $J(X)$, joille $\deg J(X) < 1$ ja

$$P(X) = Q(X)(X - c) + J(X). \quad (6.4)$$

Koska $\deg J < 1$, $J(X)$ on vakiopolynomi $J(X) = b$ jollakin $b \in K$. Erityisesti

$$0 = P(c) = Q(c)(c - c) + J(c) = b,$$

joten $b = 0$. Siis $J(X) = 0$ ja yhtälön (6.4) nojalla $(X - c) \mid P(X)$.

Toisaalta, jos $P(X) = (X - c)Q(X)$ jollain polynomilla $Q(X) \in K[X]$, niin

$$P(c) = (c - c)Q(c) = 0. \quad \square$$

Seuraus 6.17. *Olkoon K kunta. Toisen tai kolmannen asteen polynomi $P(X) \in K[X]$ on jaoton, jos ja vain jos sillä ei ole juurta kunnassa K .*

Todistus. Harjoitustehtävä 6.10 □

Esimerkki 6.18. (a) Polynomi $P(X) = X^2 + 1 \in \mathbb{C}[X]$ ei ole jaoton koska

$$X^2 + 1 = (X + i)(X - i).$$

Tämän polynomin juuret ovat $\pm i \in \mathbb{C}$. Sen sijaan Proposition 6.16 nojalla samalla lausekkeella määritellyt polynomit $P(X) \in \mathbb{Q}[X]$ ja $P(X) \in \mathbb{R}[X]$ ovat jaottomia, koska niillä ei ole juuria. Polynomi $P(X) \in \mathbb{Z}[X]$ on myös jaoton: Jos se olisi jaollinen ensimmäisen asteen polynomilla, sama pätsi myös renkaassa $\mathbb{Q}[X]$. Koska polynomin $P(X)$ korkeimman asteen kerroin on 1, niin $P(X)$ on jaollinen vain kahdella vakiopolynomilla ± 1 , jotka ovat molemmat yksiköitä.

(b) Renkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$ on neljä toisen asteen polynomia: X^2 , $X^2 + 1$, $X^2 + X$ ja $X^2 + X + 1$. Proposition 6.17 mukaan polynomi $X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ on jaoton, koska sillä ei ole yhtään juurta kahden alkion kunnassa $\mathbb{Z}/2\mathbb{Z}$, katso Harjoitustehtävä 6.4. Sen sijaan mikään muu toisen asteen polynomi ei ole jaoton tässä renkaassa: $X^2 = XX$, $X^2 + X = X(X + 1)$ ja $X^2 + 1 = (X + 1)^2$.

²Lause 6.11

Olkoon c polynomin $P(X) \in K[X]$ juuri. Jos $P(X) = (X-c)^k Q(X)$ jollain $Q(X) \in K[X]$ ja c ei ole polynomin $Q(X)$ juuri, niin c on polynomin $P(X)$ k -kertainen juuri.

Kun lasketaan polynomin $P(X)$ juuria, k -kertainen juuri lasketaan k juureksi.

Esimerkki 6.19. Polynomilla $X^2(X-1) \in \mathbb{C}[X]$ on kertaluku huomioiden kolme juurta, koska 0 on kaksinkertainen juuri.

Lause 6.20. *Olkoon K kokonaisalue ja olkoon $n \geq 0$. Jos $P(X) \in K[X] - \{0\}$ ja $\deg P(X) = n$, niin polynomilla $P(X)$ on korkeintaan n juurta.*

Todistus. Jos polynomin aste on 0, niin se on nolosta poikkeava vakiopolynomi. Tällaisella polynomilla ei ole juuria, joten väite pätee, kun $n = 0$. Oletetaan, että kaikilla $n-1$ asteen polynomeilla on korkeintaan $n-1$ juurta. Olkoon $P(X)$ polynomi, jonka aste on n . Jos polynomilla $P(X)$ on juuri $c \in K$, niin Proposition 6.16 nojalla $P(X) = (X-c)Q(X)$ jollain $Q(X) \in K[X]$. Koska K on kokonaisalue, $P(a) = 0$, jos ja vain jos $a = c$ tai $Q(a) = 0$. Proposition 6.8 mukaan $\deg(Q(X)) = n-1$ ja sillä on siis induktio-oletuksen mukaan korkeintaan $n-1$ juurta. Siis polynomilla $P(X)$ on kertaluku huomioiden korkeintaan n juurta. \square

Seuraus 6.21. *Olkoon K kokonaisalue. Olkoot $c_1, c_2, \dots, c_k \in K$ polynomin $P(X) \in K[X]$ juuria. Tällöin on $m_1, m_2, \dots, m_k \in \mathbb{N} - \{0\}$ ja $Q(X) \in K[X]$, joille pätee*

$$P(X) = (X - c_1)^{m_1} (X - c_2)^{m_2} \cdots (X - c_k)^{m_k} Q(X)$$

ja $\deg Q(X) = \deg P(X) - (m_1 + m_2 + \cdots + m_k)$. \square

Esimerkki 6.22. Lauseen 6.20 väite ei päde kaikille kommutatiivisille renkaille. Toisen asteen polynomilla $X^2 \in (\mathbb{Z}/16\mathbb{Z})[X]$ on neljä juurta: $0^2 = 4^2 = 8^2 = 12^2 = 0$. Tämän esimerkin polynomin kerroinrenkas $\mathbb{Z}/16\mathbb{Z}$ ei ole kokonaisalue.

Propositio 6.23. *Olkoon K ääretön kokonaisalue. Tällöin jokaista kokonaisalueen K polynomifunktiota vastaa yksikäsitteinen polynomi renkaassa $K[X]$.*

Todistus. Kuvaus, joka liittää polynomiin vastaavan polynomifunktion on rengashomomorfismi, joten riittää osoittaa, että tämän homomorfismin ydin on $\{0\}$. Jos polynomia $P(X)$ vastaa nollafunktio, niin sillä on äärettömän monta juurta. Lauseen 6.20 nojalla ainoa tällainen polynomi on 0. \square

Seuraus 6.24. *Olkoon K jokin kokonaisalueista \mathbb{Z} , \mathbb{Q} , \mathbb{R} tai \mathbb{C} . Kuvaus, joka liittää jokaiseen polynomiin $P(X) \in K[X]$ vastaavan polynomifunktion $P: K \rightarrow K$, on injektio.* \square

6.7 Algebrallisesti suljetut kunnat

Kunta K on **algebrallisesti suljettu**, jos jokaisella vakiosta poikkeavalla polynomilla $P(X) \in K[X]$ on juuri.

Esimerkki 6.25. (1) Reaalilukujen kunta \mathbb{R} ei ole algebrallisesti suljettu: Esimerkiksi toisen asteen polynomilla $X^2 + 1 \in \mathbb{R}[X]$ ei ole juurta.

(2) Rationaalilukujen kunta \mathbb{Q} ei ole algebrallisesti suljettu: Esimerkiksi toisen asteen polynomilla $X^2 + 1 \in \mathbb{Q}[X]$ ei ole juurta.

(3) Kahden alkion kunta $\mathbb{Z}/2\mathbb{Z}$ ei ole algebrallisesti suljettu: Esimerkiksi toisen asteen polynomilla $X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ ei ole juurta.

Lause 6.26 (Algebran peruslause). *Kompleksilukujen kunta on algebrallisesti suljettu.*

Todistus. Todistetaan kompleksianalyysin kurssilla. Toinen todistus esitetään muun muassa kurssin Lukualueet materiaalissa. \square

Lause 6.27. *Olkoon K algebrallisesti suljettu kunta. Jokainen vakiosta poikkeava polynomi $P(X) \in K[X]$ on ensimmäisen asteen polynomien tulo ja jokaisella nollasta poikkeavalla polynomilla $P(X) \in K[X]$ on juurten kertaluku huomioiden $\deg P(X)$ juurta. Polynomi $P(X) \in K[X]$ on jaoton, jos ja vain jos $\deg P(X) = 1$.*

Todistus. Todistetaan kuten Lause 6.20. \square

Seuraus 6.28. *Jokainen vakiosta poikkeava polynomi $P(X) \in \mathbb{C}[X]$ on ensimmäisen asteen polynomien tulo. Nollasta poikkeavalla polynomilla $P(X) \in \mathbb{C}[X]$ on juurten kertaluku huomioiden $\deg P(X)$ juurta.* \square

Harjoitustehtäviä

6.1. Todista Propositio 6.2.

6.2. Olkoot $P(X), Q(X) \in (\mathbb{Z}/5\mathbb{Z})[X]$,

$$P(X) = 3 + 2X + 4X^2 + 2X^3$$

ja

$$Q(X) = 4 + 4X + 4X^2 + 4X^3 + 4X^4.$$

Määritä polynomi $P(X)Q(X)$.

6.3. Laske $(1 - 2X)^8$ renkaassa $(\mathbb{Z}/16\mathbb{Z})[X]$.³

6.4. Määritä polynomien $X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$, $X^2 + X + 1 \in (\mathbb{Z}/3\mathbb{Z})[X]$ ja $X^3 + 2X + 1 \in (\mathbb{Z}/3\mathbb{Z})[X]$ juuret.

6.5. Osoita, että $1 + 2\mathbb{Z}$ on polynomien $P(X) \in (\mathbb{Z}/2\mathbb{Z})[X]$ juuri, jos ja vain jos polynomilla $P(X)$ on parillinen määrä nollasta poikkeavia kertoimia.

6.6. Todista Propositio 6.4.

6.7. Jaa polynomi

$$P(X) = X^3 + 2X^2 + 3X + 2$$

polynomilla

$$Q(X) = 2X^2 + 3X + 1$$

(1) polynomirenkaassa $\mathbb{Q}[X]$ ja

(2) polynomirenkaassa $(\mathbb{Z}/7\mathbb{Z})[X]$.

³Käytä potenssien laskusääntöjä.

6.8. Jaa polynomi

$$P(X) = X^3 + 2X^2 + X + 2 \in (\mathbb{Z}/3\mathbb{Z})[X]$$

polynomilla

$$Q(X) = X^2 + 2 \in (\mathbb{Z}/3\mathbb{Z})[X].$$

6.9. Olkoon K kokonaisalue. Olkoot $P(X), Q(X) \in K[X]$. Osoita: Jos $P(X) \mid Q(X)$ ja $Q(X) \mid P(X)$, niin on $u \in K^\times$, jolle $P(X) = uQ(X)$.

6.10. Todista Seuraus 6.17.

6.11. Anna esimerkki, joka osoittaa, että Seurauksen 6.17 väite ei päde neljännen asteen polynomeille. Päteekö Seurauksen 6.17 väite, jos oletamme vain, että K on kokonaisalue?

6.12. Mitkä polynomit $aX^2 + bX + c \in \mathbb{R}[X]$ ovat jaottomia?

6.13. (a) Onko polynomi $X^2 - 2 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?

(b) Onko polynomi $X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?

6.14. Esitä polynomi $X^5 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ jaottomien polynomien tulona.

Luku 7

Ideaalit ja kuntalaajennukset

Tässä luvussa tutustumme renkaiden ideaaleihin ja niiden avulla muodostettuihin tekijärenkaiseihin. Kurssin huipentumana sovellamme polynomirenkaiden ideaaleja kuntalaajennusten ja erityisesti äärellisten kuntien konstruktion.

7.1 Ideaalit

Olkoon G ryhmä. Olkoon $B \subset G$, $B \neq \emptyset$, vakaa osajoukko. Jos indusoidulla laskutoimituksella varustettu joukko B on ryhmä, niin se on ryhmän G aliryhmä.

Luvussa 3.5 huomasimme, että rengashomomorfismin ydin ei yleensä ole määrittelyrenkaansa alirengas. Ytimellä on kuitenkin seuraavat tärkeät ominaisuudet:

Propositio 7.1. *Olkoon $\phi: R \rightarrow R'$ rengashomomorfismi. Ydin $\ker \phi$ on additiivisen ryhmän $(R, +)$ aliryhmä. Kaikille $x \in R$ ja kaikille $a \in \ker \phi$ pätee $ax, xa \in \ker \phi$.*

Todistus. Ydin on yhteenlaskun suhteen vakaa: Jos $x, y \in \ker \phi$, niin

$$\phi(x + y) = \phi(x) + \phi(y) = 0 + 0 = 0.$$

Siis renkaan R laskutoimitus indusoi assosiativisen laskutoimituksen joukkoon $\ker \phi$. Lemman 3.20 $0 \in \ker \phi$. Jokaisella $x \in \ker \phi$ pätee $\phi(-x) = -\phi(x) = 0$ Proposition 3.7 kohdan (2) nojalla. Siis $-x \in \ker \phi$, joten $\ker \phi$ on ryhmä.

Toinen väite seuraa helposti huomaamalla, että kaikille $x \in R$ ja kaikille $a \in \ker \phi$ pätee

$$\phi(xa) = \phi(x)\phi(a) = \phi(x)0 = 0$$

ja

$$\phi(ax) = \phi(a)\phi(x) = 0\phi(x) = 0. \quad \square$$

Renkaan R epätyhjä osajoukko $\mathcal{I} \subset R$ on **ideaali**, jos

- $(\mathcal{I}, +)$ on ryhmän $(R, +)$ aliryhmä ja
- $xa, ax \in \mathcal{I}$ kaikilla $x \in R$ ja $a \in \mathcal{I}$.

Jos rengas R on kommutatiivinen, riittää tarkastaa ideaalin määritelmän ensimmäinen ehto ja kumpi tahansa jälkimmäisen ehdon tuloista.

Seuraus 7.2. Rengashomomorfismin $\phi: R \rightarrow R'$ ydin on renkaan R ideaali. \square

Esimerkki 7.3. (a) Jokaisella renkaalla R on ainakin ideaalit R ja $\{0\}$.

(b) Olkoon $\mathcal{I} \neq \{0\}$ renkaan \mathbb{Z} ideaali. Koska jokaiselle $b \in \mathcal{I}$ pätee $-b \in \mathcal{I}$, joukko $\{b \in \mathcal{I} : b > 0\}$ ei ole tyhjä. Olkoon $a = \min\{b \in \mathcal{I} : b > 0\}$. Osoitetaan, että $\mathcal{I} = a\mathbb{Z}$. Ideaalin määritelmän nojalla kaikki alkion a monikerrat ovat joukossa \mathcal{I} , joten $a\mathbb{Z} \subset \mathcal{I}$.

Olkoon $b \in \mathcal{I}$. Jakoyhtälön nojalla on $k \in \mathbb{Z}$ ja $0 \leq r < a$ siten, että $b = ka + r$. Ideaalin määritelmän nojalla $r \in \mathcal{I}$. Jos $r \neq 0$, niin $0 < r < a$, mikä on ristiriita. Siis kokonaislukujen renkaan ideaalit ovat täsmälleen joukot $a\mathbb{Z}$, $a \in \mathbb{Z}$.

Propositio 7.4 (Ideaalitestit). Olkoon R rengas. Osajoukko $A \subset R$, $A \neq \emptyset$, on ideaali, jos ja vain jos

- (1) $a - b \in A$ kaikilla $a, b \in A$ ja
- (2) $ra, ar \in A$ kaikilla $a \in A$ ja kaikilla $r \in R$.

Todistus. Harjoitustehtävä 7.1. \square

Lemma 7.5. Jos renkaan R ideaali \mathcal{I} sisältää yksikön, niin $\mathcal{I} = R$.

Todistus. Olkoon $u \in \mathcal{I}$ yksikkö. Tällöin $1 = uu^{-1} \in \mathcal{I}$. Koska \mathcal{I} on ideaali, niin kaikilla $x \in R$ pätee $x = x1 \in \mathcal{I}$, joten $\mathcal{I} = R$. \square

Propositio 7.6. Jos renkaan R ideaali \mathcal{I} on alirengas, niin $\mathcal{I} = R$.

Todistus. Jos \mathcal{I} on renkaan R alirengas, niin $1 = 1_R \in \mathcal{I}$. Väite seuraa Lemmasta 7.5. \square

Propositio 7.7. Olkoon \mathcal{I} jakorenkaan R ideaali. Silloin $\mathcal{I} = R$ tai $\mathcal{I} = \{0\}$. Erityisesti kunnan K ainoat ideaalit ovat $\{0\}$ ja K .

Todistus. Väite seuraa Lemmasta 7.5. \square

Ideaalien avulla saamme toisen todistuksen Proposition 4.8 injektiivisyysväitteelle:

Seuraus 7.8. Olkoon K kunta ja olkoon R rengas, jossa on ainakin kaksi alkioita. Olkoon $\phi: K \rightarrow R$ rengashomomorfismi. Tällöin ϕ on injektio. Erityisesti kuntahomomorfismi on injektio.

Todistus. Olkoon $\phi: R \rightarrow K$ rengashomomorfismi. Tällöin $\ker \phi$ on kunnan K ideaali. Koska $\phi(1) = 1$, pätee Proposition 7.7 nojalla $\ker \phi = \{0\}$, joten ϕ on injektio Proposition 3.23 nojalla. \square

Propositio 7.9. Olkoon $\phi: R \rightarrow S$ rengashomomorfismi. Tällöin

- (1) Jos $\mathcal{I} \subset R$ on ideaali, niin $\phi(\mathcal{I})$ on renkaan $\phi(R)$ ideaali.
- (2) Jos $\mathcal{I} \subset S$ on ideaali, niin $\phi^{-1}(\mathcal{I})$ on renkaan R ideaali.

Todistus. (1) Harjoitustehtävä 7.3.

(2) Olkoot $a, b \in \phi^{-1}(\mathcal{I})$ ja $r \in R$. Tällöin $\phi(a-b) = \phi(a) - \phi(b) \in \mathcal{I}$, koska \mathcal{I} on ideaali ja $\phi(ra) = \phi(r)\phi(a) \in \mathcal{I}$, koska $\phi(a) \in \mathcal{I}$ ja \mathcal{I} on renkaan S ideaali. Siis $ra \in \phi^{-1}(\mathcal{I})$. Vastaavasti osoitetaan, että $ar \in \phi^{-1}(\mathcal{I})$. Proposition 7.4 nojalla $\phi^{-1}(\mathcal{I})$ on ideaali. \square

Lemma 7.10. *Olkoon K kommutatiivinen rengas ja olkoon $a \in K$. Joukko*

$$(a) = Ka = \{ka : k \in K\}$$

on ideaali.

Todistus. Joukko (a) ei ole tyhjä, sillä $a \in (a)$. Jos $x, y \in (a)$, niin $x = k_1a$ ja $y = k_2a$ joillain $k_1, k_2 \in K$. Tällöin $x - y = (k_1 - k_2)a \in (a)$. Lisäksi kaikille $k \in K$ pätee $kx = (kk_1)a \in (a)$. Proposition 7.4 nojalla (a) on ideaali. \square

Olkoon K kommutatiivinen rengas. Ideaali (x) on alkion $x \in K$ virittämä **pääideaali**. Kokonaisalue, jonka kaikki ideaalit ovat pääideaaleja on **pääideaalialue**.

Lemma 7.11. *Jos K on kommutatiivinen rengas ja $u \in K^\times$, niin $(ua) = (a)$ kaikille $a \in K$.*

Todistus. Harjoitustehtävä 7.7. \square

Esimerkki 7.12. (1) Esimerkin 7.3 (b) nojalla \mathbb{Z} on pääideaalialue.

(2) Esimerkin 7.7 nojalla kaikki kunnat ovat pääideaalialueita.

Seuraavan tärkeän tuloksen todistus muistuttaa Bézout'n yhtälön¹ todistusta.

Lause 7.13. *Olkoon K kunta. Tällöin polynomirengas $K[X]$ on pääideaalialue.*

Todistus. Olkoon $\mathcal{I} \neq \{0\}$ ideaali kokonaisalueessa $K[X]$. Olkoon $B(X) \in \mathcal{I} - \{0\}$ alkio, jolle pätee $\deg(B(X)) \leq \deg(C(X))$ kaikille $C(X) \in \mathcal{I} - \{0\}$. Ideaalin määritelmän nojalla $(B(X)) \subset \mathcal{I}$.

Osoitetaan sitten, että $\mathcal{I} \subset (B(X))$. Olkoon $A(X) \in \mathcal{I}$. Jakoyhtälön mukaan on $Q(X), R(X) \in K[X]$, joille pätee $A(X) = Q(X)B(X) + R(X)$ ja $\deg(R(X)) < \deg(B(X))$. Erityisesti $R(X) = A(X) - Q(X)B(X) \in \mathcal{I}$. Koska $\deg(B(X))$ on minimaalinen nollasta poikkeaville ideaalin \mathcal{I} alkioille, pätee siis $R(X) = 0$, joten $A(X) \in (B(X))$. \square

Seurauksen 7.13 oletus, että kerronrengas on kunta on oleellinen. Esimerkiksi kokonaislukukertoimisten polynomien renkaan ideaalirakenne on monimutkaisempi:

Esimerkki 7.14. Polynomirenkaan $\mathbb{Z}[X]$ ideaali $\mathcal{I} = (2, X)$, joka koostuu niistä kokonaislukukertoimisista polynomeista, joiden vakiotermi on parillinen ei ole pääideaali: Jos $\mathcal{I} = (P(X))$ jollekin $P(X) \in \mathbb{Z}[X]$, niin $P(X)$ jakaa polynomin 2. Siis Proposition 6.8 nojalla $\deg P(X) \leq \deg 2 = 0$, koska kerronrengas \mathbb{Z} on kokonaisalue. Siis $P(X) \in \{\pm 1, \pm 2\} \subset \mathbb{Z}[X]$. Koska $X \in \mathcal{I}$, täytyy olla $P(X) = \pm 1$, joten $(P(X)) = \mathbb{Z}[X]$, mikä on ristiriita. Erityisesti siis polynomirengas $\mathbb{Z}[X]$ ei ole pääideaalirengas.

¹Propositio A.3.

7.2 Tekijärenkaat

Olkoon R rengas. Ideaalin $\mathcal{I} \subset R$ määräämä ekvivalenssirelaatio \sim määritellään aset-
tamalla $x \sim y$, jos ja vain jos $x - y \in \mathcal{I}$.^a

^aHarjoituksissa tarkastamme, että \sim on todellakin ekvivalenssirelaatio.

Propositio 7.15. *Olkoon R rengas ja olkoon $\mathcal{I} \subset R$ ideaali. Renkaan R yhteenlasku ja kertolasku ovat yhteensopivia ideaalin \mathcal{I} määräämän ekvivalenssirelaation kanssa.*

Todistus. Tarkastellaan kertolaskua: Olkoot $a, a', b, b' \in R$, $a \sim a'$ ja $b \sim b'$. Nyt $a - a' \in \mathcal{I}$ ja $b - b' \in \mathcal{I}$, joten

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in \mathcal{I},$$

koska \mathcal{I} on ideaali. Siis $ab \sim a'b'$.

Yhteenlaskun yhteensopivuus osoitetaan harjoituksissa. □

Propositio 7.15 ja Lemman 2.6 nojalla renkaan R molemmat laskutoimitukset määrittelevät tekijälaskutoimituksen tekijäjoukossa R/\mathcal{I} . Ideaalia \mathcal{I} vastaaville sivuluokille käytetään additiivista merkintää $x + \mathcal{I}$, jolloin laskutoimitukset ovat siis

$$(x + \mathcal{I}) + (y + \mathcal{I}) = (x + y) + \mathcal{I}$$

ja

$$(x + \mathcal{I})(y + \mathcal{I}) = xy + \mathcal{I}$$

kaikille $x, y \in R$. Seuraava tulos yleistää Esimerkkien 3.8(b) ja 3.21(a) tulokset kokonaislukurenkaan tilanteesta yleiseen tapaukseen:

Propositio 7.16. *Olkoon R rengas ja olkoon \mathcal{I} sen ideaali. Tällöin tekijäjoukko R/\mathcal{I} on rengas ja tekijäkuvaus $\pi: R \rightarrow R/\mathcal{I}$ on rengashomomorfismi.*

Todistus. Harjoitustehtävä 7.9. □

Seuraus 7.17. *Jokainen ideaali on jonkin rengashomomorfismin ydin.*

Todistus. Olkoon R rengas ja olkoon \mathcal{I} sen ideaali. Proposition 7.16 nojalla tekijäkuvaus $\pi: R \rightarrow R/\mathcal{I}$ on homomorfismi. Sen ydin $\pi^{-1}(0)$ on tekijärenkaan määrittelevän ekvivalenssirelaation määritelmän mukaan \mathcal{I} . □

Propositio 2.7 antaa seurauksena

Propositio 7.18. *Tekijärenkas on kommutatiivinen, jos alkuperäinen rengas on kommutatiivinen.* □

Lause 7.19 (Renkaiden isomorfismilause). *Olkoon $\psi: R \rightarrow S$ rengashomomorfismi. Tällöin tekijärenkas $R/\ker \psi$ on isomorfinen renkaan $\psi(R)$ kanssa.*

Todistus. Määritellään kuvaus $\Psi : R/\ker\psi \rightarrow \psi(R)$ asettamalla

$$\Psi(x + \ker\psi) = \psi(x)$$

kaikille $x + \ker\psi \in R/\ker\psi$. Tarkastetaan, että kuvaus Ψ on hyvin määritelty, mikä tarkoittaa, että sen arvo ei riipu kuvattavan ekvivalenssiluokan edustajan valinnasta. Jos $x + \ker\psi = y + \ker\psi$, niin $x \sim y$, mikä määritelmän mukaan tarkoittaa $x - y \in \ker\psi$. Siis $\psi(x) - \psi(y) = \psi(x - y) = 0$, joten

$$\Psi(x + \ker\psi) = \psi(x) = \psi(y) = \Psi(y + \ker\psi).$$

Osoitetaan, että Ψ on rengashomomorfismi: Olkoot $x, y \in R$. Tällöin

$$\begin{aligned} \Psi(x + \ker\psi) + \Psi(y + \ker\psi) &= \psi(x) + \psi(y) = \psi(x + y) = \Psi(x + y + \ker\psi) \\ &= \Psi(x + \ker\psi + y + \ker\psi), \end{aligned}$$

$$\begin{aligned} \Psi(x + \ker\psi)\Psi(y + \ker\psi) &= \psi(x)\psi(y) = \psi(xy) = \Psi(xy + \ker\psi) \\ &= \Psi((x + \ker\psi)(y + \ker\psi)) \end{aligned}$$

ja $\Psi(1 + \ker\psi) = \psi(1) = 1$, koska ψ on rengashomomorfismi.

Kuvaus Ψ on määritelmänsä nojalla surjektio. Osoitetaan se vielä injektiksi, jolloin väite tulee todistetuksi. Olkoon $x + \ker\psi \in \ker\Psi$. Tällöin $\psi(x) = 0$, joten $x \in \ker\psi$. Siis $x + \ker\psi = 0 + \ker\psi = 0 \in R/\ker\psi$. Siis Ψ on injektio. \square

Seuraus 7.20. *Kunnalla, jonka karakteristika on p on alikunta, joka on isomorfinen kunnan $\mathbb{Z}/p\mathbb{Z}$ kanssa.*

Todistus. Olkoon K kunta, jonka karakteristika on p . Olkoon $\phi: \mathbb{Z} \rightarrow K$ rengashomomorfismi. Karakteristikan määritelmän nojalla $\ker\phi = p\mathbb{Z}$, joten isomorfismilauseen nojalla $\phi(\mathbb{Z})$ on isomorfinen kunnan $\mathbb{Z}/p\mathbb{Z}$ kanssa. \square

Esimerkki 7.21. (a) Koska R on aina renkaan R ideaali ja $R/R \cong \{0\}$, niin tekijärenkas R/\mathcal{I} voi olla kommutatiivinen vaikka R ei olisikaan. Toinen ääriesimerkki tekijärenkaasta on $R/\{0\} \cong R$.

(b) Olkoon $\Omega \neq \emptyset$ ja olkoon R rengas. Esimerkissä 3.21 tarkasteltu evaluaatiohomomorfismi $E_c: \mathcal{F}(\Omega, R) \rightarrow R$ on surjektio kaikille $c \in \Omega$, koska $E_c(\underline{a}) = a$ kaikille $a \in R$. Renkaiden isomorfismilauseen nojalla $\mathcal{F}(\Omega, R)/\ker E_c$ on rengasisomorfinen renkaan R kanssa kaikille $c \in \Omega$.

(c) Reaaliluvut konstruoidaan kurssilla Lukualueet (katso [LA], luku 5) rationaalilukujen Cauchyn jonojen renkaan nollaan suppenevien jonojen ideaalia vastaavana tekijärenkaana.

Lause 7.22. *Olkoon K kunta ja olkoon $P(X) \in K[X]$ polynomi, jonka aste on $d \geq 1$. Jos kunnassa K on q alkioita, niin renkaassa $K[X]/(P(X))$ on q^d alkioita.*

Todistus. Polynomien jakoyhtälön² nojalla jokaisella tekijärenkaan $K[X]/(P(X))$ alkiolla $Q(X) + (P(X)) \in K[X]/(P(X))$ on edustaja $\overline{Q}(X)$, jolle pätee $\deg \overline{Q}(X) < \deg P(X) = d$:

$$Q(X) = T(X)P(X) + \overline{Q}(X)$$

yksikäsitteiselle $T(X) \in K[X]$. Tällaisia polynomeja on q^d kappaletta ja mitkään kaksi eivät ole ekvivalentteja. \square

²Seuraus 6.12

Esimerkki 7.23. Olkoon $P(X) = X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$. Lauseen 7.22 todistuksesta seuraa, että renkaan $(\mathbb{Z}/2\mathbb{Z})[X]/(P(X))$ alkiot ovat

$$\begin{aligned} 0 &= (P(X)), & 1 &= 1 + (P(X)), \\ \alpha &= X + (P(X)) \quad \text{ja} \quad \alpha + 1 &= X + 1 + (P(X)). \end{aligned}$$

Tekijärenkaan yhteen- ja kertolaskun laskutaulut ovat

+	0	1	α	$\alpha + 1$		·	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$		0	0	0	0	0
1	1	0	$\alpha + 1$	α	ja	1	0	1	α	$\alpha + 1$
α	α	$\alpha + 1$	0	1		α	0	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	α	1	0		$\alpha + 1$	0	$\alpha + 1$	1	α

Laskutaulusta on helppo tarkastaa, että $(\mathbb{Z}/2\mathbb{Z})[X]/(P(X))$ on kunta. Laskutauluja vertaamalla näemme, että kunta $(\mathbb{Z}/2\mathbb{Z})[X]/(P(X))$ on isomorfinen Esimerkissä 4.6 tarkastellun kunnan F kanssa, siellähän $\beta = \alpha + 1$.

7.3 Maksimaaliset ideaalit

Olkoon R rengas. Renkaan R ideaali \mathcal{I} on **aito**, jos $\mathcal{I} \neq R$. Renkaan R aito ideaali \mathcal{M} on **maksimaalinen ideaali**, jos se ei ole minkään aidon ideaalin aito osajoukko.

Proposition 7.7 mukaan kunnan nollaideaali on maksimaalinen ideaali.

Propositio 7.24. *Kokonaislukurenkaan ideaali $q\mathbb{Z}$, $q \geq 2$, on maksimaalinen, jos ja vain jos q on alkuluku.*

Todistus. Jos q ei ole alkuluku, niin $q = ab$ joillakin $a, b \in \mathbb{N} - \{0, 1\}$. Tällöin $q \in a\mathbb{Z}$, joten ideaali $q\mathbb{Z}$ sisältyy aidosti aitoon ideaaliin $a\mathbb{Z}$ eikä $q\mathbb{Z}$ siis ole maksimaalinen.

Olkoon q alkuluku ja olkoon $r\mathbb{Z}$ ideaali, joka sisältää aidosti ideaalin $q\mathbb{Z}$. Siis $r \neq \pm q$. Erityisesti $q \in r\mathbb{Z}$ ja koska q on alkuluku, pitää olla $r = \pm 1$. Siis $r\mathbb{Z} = \mathbb{Z}$. \square

Lauseen 5.19 mukaan tekijärenkas $\mathbb{Z}/q\mathbb{Z}$ on kunta täsmälleen silloin, kun q on alkuluku. Proposition 7.24 mukaan tämä on yhtäpitävää sen kanssa, että $q\mathbb{Z}$ on kokonaislukurenkaan maksimaalinen ideaali. Seuraava tulos yleistää tämän havainnon.

Lause 7.25. *Olkoon \mathcal{M} kommutatiivisen renkaan K maksimaalinen ideaali. Tällöin tekijärenkas K/\mathcal{M} on kunta.*

Todistus. Proposition 7.18 nojalla tekijärenkas K/\mathcal{M} on kommutatiivinen. Koska \mathcal{M} on renkaan K aito osajoukko, niin tekijärenkaassa K/\mathcal{M} on ainakin kaksi alkioita. Olkoon $a + \mathcal{M} \in K/\mathcal{M} - \{0\}$. Harjoitustehtävässä 7.12 osoitetaan, että

$$\mathcal{N} = \{ak + m : k \in K, m \in \mathcal{M}\}$$

on renkaan K ideaali. Ideaali \mathcal{N} sisältää aidosti ideaalin \mathcal{M} , koska $a \in \mathcal{N} - \mathcal{M}$. Koska \mathcal{M} on maksimaalinen, pätee $\mathcal{N} = K$. Erityisesti $1 \in \mathcal{N}$, joten on $k \in K$ ja $m \in \mathcal{M}$ siten, että $ak + m = 1$. Mutta tästä saadaan

$$(a + \mathcal{M})(k + \mathcal{M}) = ak + \mathcal{M} = 1 - m + \mathcal{M} = 1 \in K/\mathcal{M},$$

joten $a + \mathcal{M}$ on yksikkö. \square

Seuraava tulos antaa keinon maksimaalisten ideaalien tunnistamiseen pääideaalialueissa.

Lause 7.26. *Olkoon K pääideaalialue ja olkoon $a \in K - \{0\}$. Tällöin pääideaali (a) on maksimaalinen ideaali, jos ja vain jos a on jaoton.*

Todistus. Olkoon a jaoton ja olkoon \mathcal{N} ideaali, joka sisältää pääideaalin (a) . Koska K on pääideaalialue, niin $\mathcal{N} = (b)$ jollain $b \in K$. Pätee siis $a = qb$ jollain $q \in K$. Koska a on jaoton, täytyy olla $q \in K^\times$ tai $b \in K^\times$. Jos q on yksikkö, niin Lemman 7.11 nojalla $\mathcal{N} = (b) = (qb) = (a)$. Jos taas b on yksikkö, niin Lemman 7.5 nojalla $\mathcal{N} = (b) = K$. Siis (a) on maksimaalinen.

Toinen suunta osoitetaan Harjoitustehtävässä 7.13. □

7.4 Kuntalaajennukset polynomirenkaiden avulla

Seuraus 7.27. *Olkoon K kunta ja olkoon $P(X) \in K[X]$ jaoton. Tällöin $(P(X))$ on maksimaalinen ideaali.*

Todistus. Polynomirengas $K[X]$ on pääideaalialue Lauseen 7.13 nojalla, joten väite seuraa Lauseesta 7.26. □

Seuraus 7.28. *Olkoon K kunta ja olkoon $P(X) \in K[X]$ jaoton. Tällöin tekijärengas $K[X]/(P(X))$ on kunta.*

Todistus. Väite seuraa Lauseesta 7.25 ja Seurauksesta 7.27. □

Esimerkki 7.29. Esimerkissä 6.18 osoitimme, että polynomi $P(X) = X^2 + X + 1$ on jaoton toisen asteen polynomi polynomirenkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$. Seurauksen 7.28 ja Lauseen 7.22 nojalla $\mathbb{F}_4 = (\mathbb{Z}/2\mathbb{Z})[X]/(P(X))$ on neljän alkion kunta. Totesimme saman laskutauluja tarkastelemalla Esimerkissä 7.23.

Esimerkin 7.23 lisäksi olemme tavanneet äärelliset kunnat $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, missä p on alkuluku. Erityisesti näiden kuntien alkioiden lukumäärä on alkuluku. Esimerkin 7.23 tulos yleistyy kaikille alkulukupotensseille p^q .

Lause 7.30. *Jokaiselle luonnolliselle luvulle $q \geq 1$ ja alkuluvulle p on äärellinen kunta, jossa on p^q alkioita. Toisaalta jokaisessa äärellisessä kunnassa on p^q alkioita joillain tällaisilla p ja q .*

Todistus. Lauseen 5.10 mukaan äärellisessä kunnassa on p^q alkioita jollain alkuluvulla p ja jollain luonnollisella luvulla $q \geq 1$. Emme osoita tällä kurssilla äärellisen kunnan olemassaoloa yleisessä tapauksessa. Koko lauseen todistus on esimerkiksi lähteissä [DF, Luku 14.3], [IR, Luku 7.2] ja [War, Luku39] ja kurssilla Äärelliset kunnat. Harjoitustehtävissä tehdään muutamia muita erikoistapauksia. □

Esimerkki 7.31. Polynomi $X^2 + 1$ on jaoton polynomirenkaassa $(\mathbb{Z}/p\mathbb{Z})[X]$ kaikilla alkuluvuilla $p \equiv 3 \pmod{4}$. Todistamme tämän kurssilla RYHMÄT ryhmäteorian Lagrangen lauseen avulla Lemmana 11.20. Kunnassa $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1)$ on p^2 alkioita näillä alkuluvuilla p . Toisaalta $X^2 + 1$ ei ole jaoton, jos $p \equiv 1 \pmod{4}$. Emme todista tätä väitettä mutta se on helppo tarkastaa esimerkiksi alkulukujen 5, 13 ja 17 tapauksissa. Aihetta käsitellään yksityiskohtaisesti esimerkiksi lähteessä [IR, Luku 5].

Seuraava tulos osoittaa, että kuntakertoimisesta polynomirenkaasta $K[X]$ saadaan jaottoman polynomin avulla muodostettua tarkasteltavan kerroinkunnan kuntalaajennus k . Konstruktiossa käytetyillä polynomilla $P(X) \in K[X]$ ei ole juuria Proposition 6.16 nojalla. Kun polynomin $P(X)$ kertoimet ajatellaan uuden kunnan alkioiksi samastamalla K vakiopolynomien antaman alikunnan kanssa, havaitaan, että polynomilla $P(X) \in k[X]$ on juuri.

Seuraus 7.32. *Olkkoon K kunta ja olkkoon $P(X) \in K[X]$ jaoton. Tällöin kunnalla $k = K[X]/(P(X))$ on alikunta, joka on isomorfinen kunnan K kanssa. Polynomilla $P(X) \in k[X]$ on juuri.*

Todistus. Olkkoon $i: K \rightarrow K[X]$ homomorfismi, joka kuvaa alkion $a \in K$ polynomiksi $a \in K[X]$ ja olkkoon $\Phi: K[X] \rightarrow K[X]/(P(X))$ luonnollinen homomorfismi. Propositioiden 6.2 ja 7.16 mukaan kuvaus $\Phi \circ i$ on homomorfismi kunnasta renkaaseen, jossa on ainakin 2 alkioita, joten se on injektio Proposition 4.8 nojalla. Ensimmäinen väite seuraa tästä.

Osoitetaan vielä, että polynomilla

$$P(X) = \sum_{k=0}^n b_k X^k \in k[X]$$

on juuri. Olkkoon

$$\alpha = \Phi(X) = X + (P(X)) \in k.$$

Tällöin pätee

$$\begin{aligned} P(\alpha) &= P(X + (P(X))) = \sum_{k=0}^n (b_k + (P(X))(X + (P(X))))^k \\ &= \sum_{k=0}^n (b_k + (P(X))(X^k + (P(X)))) = P(X) + (P(X)) = 0, \end{aligned}$$

joten α on polynomin $P(X) \in k[X]$ juuri. □

Esimerkki 7.33. Polynomi $X^2 + 1 \in \mathbb{R}[X]$ on jaoton, koska sillä ei ole juurta. Tekijärenkas $k = \mathbb{R}[X]/(X^2 + 1)$ on Seurauksen 7.32 nojalla kunta ja polynomilla $X^2 + 1 \in k[X]$ on juuri.

Reaalikertoimisten polynomien renkas $\mathbb{R}[X]$ on kompleksikertoimisten polynomien renkaan $\mathbb{C}[X]$ alirengas ja Seurauksen 6.24 nojalla reaalikertoimiset polynomit voidaan samastaa kompleksitasossa määriteltyjen reaalikertoimisten polynomifunktioiden renkaan kanssa.

Olkkoon $E_i: \mathbb{C}[X] \rightarrow \mathbb{C}$ Esimerkissä 3.21 määritelty evaluaatiokuvaus

$$E_i(P(X)) = P(i).$$

Proposition 6.16 nojalla $\ker E_i = (X - i)$. Rajoittumakuvaus $E_i|_{\mathbb{R}[X]}: \mathbb{R}[X] \rightarrow \mathbb{C}$ on surjektiivinen rengashomomorfismi, koska $E_i(bX + a) = a + ib$ kaikilla $a, b \in \mathbb{R}$.

Harjoitustehtävän 7.18 mukaan $-i$ on jokaisen sellaisen polynomin $P(X) \in \mathbb{C}[X]$ juuri, jonka kertoimet ovat reaalisia ja jonka yksi juuri on i . Siis jokainen homomorfismin $E_i|_{\mathbb{R}[X]}$ ytimeen kuuluva polynomi on jaollinen polynomilla $X^2 + 1 = (X - i)(X + i)$, joten $\ker E_i|_{\mathbb{R}[X]} = (X^2 + 1)$. Renkaiden isomorfismilauseen mukaan kunta $\mathbb{R}[X]/(X^2 + 1)$ on isomorfinen kompleksilukujen kunnan \mathbb{C} kanssa.

Esimerkki 7.34. Polynomirenkaan $\mathbb{C}[X]$ maksimaaliset ideaalit ovat Seurauksen 7.27 mukaan jaottomien polynomien virittämät pääideaalit. Algebran peruslauseeseen nojalla \mathbb{C} on algebrallisesti suljettu, joten $P(X) \in \mathbb{C}[X]$ on jaoton, jos ja vain jos $\deg P(X) = 1$. Jos $\deg P(X) = 1$, niin $P(X) = aX + b$ joillakin $a \in \mathbb{C}^\times$ ja $b \in \mathbb{C}$. Lemman 7.11 mukaan polynomirenkaan $P(X) \in \mathbb{C}[X]$ maksimaaliset ideaalit ovat pääideaalit $(X - c) = \ker E_c$, $c \in \mathbb{C}$. Evaluaatiokuvaus $E_c: \mathbb{C}[X] \rightarrow \mathbb{C}$ on surjektiivinen rengashomomorfismi, joten renkaiden isomorfismilauseeseen nojalla tekijärenkas $\mathbb{C}[X]/(X - c)$ on isomorfinen kompleksilukujen kunnan \mathbb{C} kanssa.

Harjoitustehtäviä

7.1. Todista Propositio 7.4.

7.2. Olkoon R rengas ja olkoon \mathcal{I} renkaan R epätyhjä osajoukko. Osoita, että \mathcal{I} on ideaali, jos ja vain jos $xa + x'a', ax + a'x' \in \mathcal{I}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathcal{I}$.

7.3. Todista Propositio 7.9(1).

7.4. Anna esimerkki, joka osoittaa, että Proposition 7.9(1) tilanteessa $\psi(\mathcal{I})$ ei välttämättä ole renkaan S ideaali.

7.5. Olkoot \mathcal{I}_i , $i \in I$, renkaan R ideaaleja. Osoita, että $\bigcap_{i \in I} \mathcal{I}_i$ on renkaan R ideaali.

7.6. Olkoon K kommutatiivinen rengas. Olkoot $a_1, a_2, \dots, a_n \in K$. Osoita, että

$$\{x_1 a_1 + x_2 a_2 + \dots + x_n a_n : x_1, x_2, \dots, x_n \in K\}$$

on renkaan K ideaali.

7.7. Todista Lemma 7.11.

7.8. Olkoon R rengas ja olkoon $\mathcal{I} \subset R$ ideaali. Asetetaan $x \sim y$, jos ja vain jos $x - y \in \mathcal{I}$. Osoita, että \sim on ekvivalenssirelaatio.

7.9. Todista Lemma 7.16.

7.10. Osoita, että $\mathcal{I} = \{0, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$ on renkaan $\mathbb{Z}/6\mathbb{Z}$ ideaali. Osoita, että tekijärenkas $(\mathbb{Z}/6\mathbb{Z})/\mathcal{I}$ on rengasisomorfinen renkaan $\mathbb{Z}/2\mathbb{Z}$ kanssa.

7.11. Määritä tekijärenkaan $R = (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + 1)$ laskutaulut. Mitkä renkaan R alkioit ovat yksiköitä? Onko rengas R kunta?

7.12. Olkoon \mathcal{I} kommutatiivisen renkaan K ideaali ja olkoon $a \in K$. Osoita, että

$$\mathcal{N} = \{ak + m : k \in K, m \in \mathcal{I}\}$$

on renkaan K ideaali.

7.13. Olkoon K kokonaisalue ja olkoon $a \in K - \{0\}$ alkio, joka ei ole jaoton. Osoita, että (a) ei ole maksimaalinen ideaali.

7.14. Osoita, että polynomi $X^3 + X^2 + X + 2 \in (\mathbb{Z}/3\mathbb{Z})[X]$ on jaoton. Osoita tämän avulla, että on kunta, jossa on 27 alkioita.

7.15. Anna esimerkki jaottomasta toisen asteen polynomista polynomirenkaassa $(\mathbb{Z}/3\mathbb{Z})[X]$. Osoita tämän avulla, että on kunta, jossa on 9 alkioita.

- 7.16. Osoita, että on sellainen kunta, jossa on täsmälleen 16 alkioita.³
- 7.17. Osoita, että on kunta, jossa on 125 alkioita.
- 7.18. Olkoot $a_k \in \mathbb{R}$ kaikilla $k \in \{0, 1, 2, \dots, n\}$ ja olkoon $z_0 \in \mathbb{C}$ yhtälön

$$\sum_{k=0}^n a_k z^k = 0 \quad (7.1)$$

ratkaisu. Osoita, että \bar{z}_0 on yhtälön (7.1) ratkaisu. Päteekö väite, jos oletetaan vain, että $a_k \in \mathbb{C}$ kaikilla $k \in \{0, 1, 2, \dots, n\}$

Kommutatiivisen renkaan K ideaali $\mathcal{P} \neq K$ on **alkuideaali**, jos sillä on seuraava ominaisuus: Jos $a, b \in K$ ja $ab \in \mathcal{P}$, niin $a \in \mathcal{P}$ tai $b \in \mathcal{P}$.

- 7.19. Mitkä kokonaislukujen renkaan ideaalit ovat alkuideaaleja?
- 7.20. Olkoon K kommutatiivinen rengas ja olkoon $\mathcal{I} \neq K$ sen ideaali. Osoita, että tekijärengas K/\mathcal{I} on kokonaisalue, jos ja vain jos \mathcal{I} on alkuideaali.
- 7.21. Osoita, että kommutatiivisen renkaan jokainen maksimaalinen ideaali on alkuideaali.
- 7.22. Osoita, esimerkiksi, että kommutatiivisen renkaan alkuideaali ei välttämättä ole maksimaalinen.

³Muista Harjoitustehtävät 6.10 ja 6.14.

Osa III

Ryhmät

Luku 8

Ryhmät

Tässä luvussa tarkastelemme laskutoimituksella varustettuja joukkoja, joiden laskutoimitukselta oletamme muutamia yksinkertaisia ominaisuuksia. Näin määriteltävä ryhmän käsite on tärkeä esimerkiksi geometriassa ja lukuteoriassa. Ryhmiä käsiteltiin lyhyesti myös kurssilla RENKAAT JA KUNNAT luvussa 3.2 koska kommutatiivisen ryhmän käsite esiintyy renkaan määritelmässä.

8.1 Ryhmä

Laskutoimituksella varustettu joukko^a $(G, *)$ on **ryhmä**, jos

- laskutoimitus $*$ on assosiatiivinen,
- laskutoimituksella $*$ on neutraalialkio,
- jokaisella $g \in (G, *)$ on käänteisalkio.

Ryhmän G alkioden lukumäärä $\#G$ on ryhmän G **kertaluku**.

^aMuista määritelmä luvusta 1.1.

Ryhmä on keskeinen algebran rakenne, joka esiintyy monilla matematiikan aloilla esimerkiksi lineaarialgebrassa, geometriassa ja lukuteoriassa. Tällä kurssilla käsittelemme esimerkkejä eri aloilta yleisen teorian tarkastelun lisäksi.

Esimerkki 8.1. Esimerkkien 1.9 ja 1.17 nojalla laskutoimituksella varustetut joukot $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, kongruenssiluokkien additiivinen ryhmä $(\mathbb{Z}/p\mathbb{Z}, +)$ ¹ ja multiplikatiiviset ryhmät

$$\mathbb{Z}^\times = (\{-1, 1\}, \cdot), \quad \mathbb{Q}^\times = (\mathbb{Q} - \{0\}, \cdot), \quad \mathbb{R}^\times = (\mathbb{R}, \cdot) \text{ ja } \mathbb{C}^\times = (\mathbb{C} - \{0\}, \cdot)$$

ovat ryhmiä.

¹Katso luvut 2.1 ja 2.3.

Kurssilla RENKAAT JA KUNNAT käsitellään näiden esimerkkien yleistyksiä, renkaan R additiivista ryhmää $(R, +)$ ja yksiköiden ryhmää eli multiplikatiivista ryhmää R^\times , jonka laskutoimitus on renkaan R kertolasku.

Esimerkki 8.2. Olkoon $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}^2$ ja olkoon $n \in \mathbb{N} - \{0, 1\}$. Lineaarialgebran kurssilla osoitetusta determinantin laskusäännöstä $\det AB = \det A \det B$ seuraa, että joukko $\{A \in M_n(\mathbb{K}) : \det A \neq 0\}$ on laskutoimituksella varustetun joukon $(M_n(\mathbb{K}), \cdot)$ vakaa osajoukko ja matriisien kertolasku indusoi laskutoimituksen tähän joukkoon. Matriisien kertolasku on lineaarialgebran tietojen nojalla assosiatiivinen ja identtinen matriisi I_n on tämän laskutoimituksen neutraalialkio.

Jos $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$,³ niin jokaisella matriisilla $A \in M_n(\mathbb{K})$, jonka determinantti ei ole 0, on käänteismatriisi $A^{-1} \in M_n(\mathbb{K})$, jonka determinantti on $1/\det A \neq 0$. Käänteismatriisi A^{-1} on alkion A käänteisalkio matriisien kertolaskun indusoimalla laskutoimituksella varustetussa joukossa $\{A \in M_n(\mathbb{K}) : \det A \neq 0\}$, joka on siis ryhmä.

Olkoon \mathbb{K} kunta. Matriisien kertolaskulla varustettu joukko

$$\mathrm{GL}_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) : \det A \neq 0\}$$

on \mathbb{K} -kertoiminen yleinen lineaarinen ryhmä.

Esimerkki 8.3. Matriisien kertolaskulla varustettu joukko $\{A \in M_n(\mathbb{Z}) : \det A \neq 0\}$ on yleisen lineaarisen ryhmän $\mathrm{GL}_n(\mathbb{Q})$ vakaa osajoukko mutta se ei ole ryhmä: Matriisin $D = \mathrm{diag}(2, 2, \dots, 2)$ determinantti on $2^n \neq 0$, joten matriisilla D on rationaalisessa yleisessä lineaarisessa ryhmässä käänteismatriisi

$$D^{-1} = \mathrm{diag}(1/2, 1/2, \dots, 1/2) \in \mathrm{GL}_2(\mathbb{Q}).$$

Käänteismatriisi on yksikäsitteinen, joten matriisilla D ei ole käänteismatriisia laskutoimituksella varustetussa joukossa $\{A \in M_n(\mathbb{Z}) : \det A \neq 0\}$. Harjoituksissa osoitetaan, että

$$\mathrm{SL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det A = 1\}$$

on ryhmä.

Olkoon \mathbb{K} kokonaisalue. Matriisien kertolaskulla varustettu joukko

$$\mathrm{SL}_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) : \det A = 1\}$$

on \mathbb{K} -kertoiminen erityinen lineaarinen ryhmä.

Ryhmän laskutoimitus jätetään usein mainitsematta ja puhutaan vain "ryhmästä G ". Tällöin laskutoimitus on kuitenkin kiinnitetty ja usein konkreettisessa tilanteessa se on ennalta tiedossa.

Puhuttaessa abstraktisti ryhmästä G merkitään laskutoimitusta usein kuten kertolaskua ja neutraalialkiolle käytetään merkintää e tai joskus myös merkintää 1. Tällöin ryhmää G kutsutaan multiplikatiiviseksi ryhmäksi.

²Riittää, että K on kokonaisalue, katso lisää luvuissa 4 ja 5.

³Riittää, että \mathbb{K} on kunta, katso luku 4.

Jos tarkastellaan useampia ryhmiä samalla kertaa voidaan niiden neutraalialkioille käyttää ryhmille käytettävien merkintöjen kanssa yhteensopivaa merkintää esimerkiksi niin, että esimerkiksi ryhmän G' neutraalialkiota merkitään e' . Joskus tehdään toisenlaisiakin valintoja.

Propositio 8.4. *Olkoon G ryhmä, jonka neutraalialkio on e . Tällöin*

- (1) *Neutraalialkio e on yksikäsitteinen.*
- (2) *Jokaisen alkion käänteisalkio on yksikäsitteinen.*
- (3) *Jos $\bar{a}a = e$, niin \bar{a} on alkion a käänteisalkio.*
- (4) *$(ab)^{-1} = b^{-1}a^{-1}$ kaikilla $a, b \in G$.*

Todistus. (1) Propositio 1.13.

(2) Olkoot $a, b, c \in G$ siten, että $ab = e = ca$. Tällöin $b = eb = cab = ce = c$.

(3) Alkiolla a on käänteisalkio a^{-1} . Oletuksesta seuraa $\bar{a} = \bar{a}(aa^{-1}) = (\bar{a}a)a^{-1} = a^{-1}$.

(4) Koska pätee

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e,$$

niin väite seuraa kohdasta (3). □

Propositio 8.4(3) helpottaa käänteisalkion etsimistä ryhmässä: riittää tarkastaa, että alkio on vasen tai oikea käänteisalkio.

Supistussäännöt ovat voimassa laskutoimituksella varustetussa joukossa $(A, *)$, jos kaikilla $a, b, c \in A$ pätee

- (1) Jos $a * b = a * c$, niin $b = c$.
- (2) Jos $a * b = c * b$, niin $a = c$.

Propositio 8.5. *Supistussäännöt pätevät ryhmässä.*

Todistus. Olkoon G ryhmä ja olkoot $a, b, c \in G$ siten, että $ab = ac$. Siis

$$b = a^{-1}(ab) = a^{-1}(ac) = c,$$

joten sääntö (1) pätee. Sääntö 2 todistetaan samaan tapaan. □

Propositio 8.6. *Olkoon A assosiatiivisella laskutoimituksella varustettu joukko, jossa on neutraalialkio. Tällöin A on ryhmä, jos ja vain jos yhtälöillä $ax = b$ ja $ya = b$ on ratkaisu joukossa A kaikilla $a, b \in A$.*

Todistus. Harjoitustehtävä 8.5. □

Lemma 8.7. *Äärellisen ryhmän laskutaulussa⁴ jokaisella rivillä ja jokaisessa sarakkeessa esiintyvät kaikki ryhmän alkio.*

Todistus. Harjoitustehtävä 8.6. □

⁴Katso luku 1.1. Ryhmän laskutaulua kutsutaan usein kertotauluksi, jos laskutoimitus ei ole $+$.

Esimerkki 8.8. Neljän alkion ryhmän $\mathbb{Z}/4\mathbb{Z}$, laskutaulu on

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Laskutaulussa käytetään kongruenssiluokan $k + 4\mathbb{Z}$ merkintänä edustajaa $k \in \mathbb{Z}$.

Ryhmä G on **kommutatiivinen ryhmä** eli **Abelin ryhmä**, jos sen laskutoimitus on kommutatiivinen.

Kommutatiivisen ryhmän laskutoimituksen merkinä on joskus $+$. Ryhmää $(G, +)$ kutsutaan usein **additiiviseksi ryhmäksi**.

Merkintää $+$ käytetään ainoastaan kommutatiiviselle laskutoimitukselle.

Esimerkki 8.9. (a) Ryhmät \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} ja $\mathbb{Z}/q\mathbb{Z}$ ovat kommutatiivisia.

(b) Erityinen lineaarinen ryhmä $SL_n(\mathbb{R})$ ei ole kommutatiivinen, katso Esimerkki 1.9.

Esimerkki 8.10. Reaalinen⁵ vektoriavaruus (eli \mathbb{R} -vektoriavaruus) muodostuu kommutatiivisesta ryhmästä $(V, +)$, jossa on määritelty alkioiden yhteenlaskun kanssa yhteensopiva kertominen reaaliluvulla. Reaaliluvulla kertominen tarkoittaa kuvausta $\mathbb{R} \times V \rightarrow V$, $(\lambda, v) \mapsto \lambda v$. Laskutoimitukselta ja reaaliluvulla kertomiselta oletetaan

- (1) $\lambda(v + w) = \lambda v + \lambda w$ kaikille $\lambda \in \mathbb{R}$ ja $v, w \in V$,
- (2) $(\lambda + \mu)v = \lambda v + \mu v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$,
- (3) $\mu(\lambda v) = (\mu\lambda)v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$ ja
- (4) $1v = v$ kaikille $v \in V$.

Esimerkki 8.11. Olkoon $X \neq \emptyset$ ja olkoon

$$\mathcal{F}(X) = \{f: X \rightarrow X\}.$$

Esimerkissä 1.11 havaitsimme, että laskutoimitus \circ on assosiatiiivinen ja että se ei ole kommutatiivinen, jos joukossa X on ainakin kaksi alkioita.

Osajoukko $\{f: X \rightarrow X : f \text{ on bijektio}\} \subset \mathcal{F}(X)$ on vakaa, koska tunnetusti kahden bijektio yhdistetty kuvaus on bijektio. Siis laskutoimitus \circ määrää laskutoimituksen bijektioiden muodostamassa osajoukossa. Edellä tekemämme havainnot osoittavat, että joukon X bijektiot itselleen muodostavat ryhmän.

Olkoon X epätyhjä joukko. Laskutoimituksella varustettu joukko

$$\text{Perm}(X) = (\{f: X \rightarrow X : f \text{ on bijektio}\}, \circ)$$

on joukon X **permutaatioryhmä**.

Ryhmän $\text{Perm}(X)$ alkiot ovat joukon X **permutaatioita**.

⁵Tämä esimerkki pätee yleisessä kuntakertoimisessa vektoriavaruudessa, katso luku 4.4.

8.2 Ryhmien suora tulo

Olkoon $A \neq \emptyset$ indeksijoukko ja olkoot G_α ryhmiä kaikilla $\alpha \in A$. Ryhmien G_α , $\alpha \in A$, suora tulo $\prod_{\alpha \in A} G_\alpha$ on joukko

$$\prod_{\alpha \in A} G_\alpha = \left\{ (g_\alpha)_{\alpha \in A} : g_\alpha \in G_\alpha \text{ kaikilla } \alpha \in A \right\}$$

varustettuna komponenteittaisella laskutoimituksella:

$$(gh)_\alpha = g_\alpha h_\alpha$$

kaikilla $\alpha \in A$ kaikilla $g, h \in \prod_{\alpha \in A} G_\alpha$.

Propositio 8.12. *Olkoon $A \neq \emptyset$ indeksijoukko ja olkoot G_α ryhmiä kaikilla $\alpha \in A$. Tällöin $\prod_{\alpha \in A} G_\alpha$ on ryhmä. Jos kaikki ryhmät G_α , $\alpha \in A$, ovat kommutatiivisia, niin $\prod_{\alpha \in A} G_\alpha$ on kommutatiivinen ryhmä.*

Todistus. Olkoot $g = (g_\alpha)_{\alpha \in A}$, $h = (h_\alpha)_{\alpha \in A}$, $k = (k_\alpha)_{\alpha \in A} \in \prod_{\alpha \in A} G_\alpha$. Ryhmän G_β laskutoimituksen assosiativisuuden nojalla

$$(g(hk))_\beta = g_\beta(h_\beta k_\beta) = (g_\beta h_\beta)k_\beta = ((gh)k)_\beta$$

kaikille $\beta \in A$. Siis tulojoukon laskutoimitus on assosiativinen. Jos $e_\alpha \in G_\alpha$ on neutraalialkio, niin $(e_\alpha)_{\alpha \in A}$ on neutraalialkio laskutoimituksella varustetussa joukossa $\prod_{\alpha \in A} G_\alpha$. Alkion $(g_\alpha)_{\alpha \in A}$ käänteisalkio on $(g_\alpha^{-1})_{\alpha \in A}$.

Oletetaan, että kaikki ryhmät G_α , $\alpha \in A$ ovat kommutatiivisia. Ryhmän G_β laskutoimituksen kommutatiivisuuden nojalla

$$(gh)_\beta = g_\beta h_\beta = (h_\beta g_\beta) = (gh)_\beta$$

kaikille $\beta \in A$. Siis tulojoukon laskutoimitus on kommutatiivinen. □

Äärellisen monen ryhmän suora tulo on helpompi hahmottaa kuin yleinen määritelmä. Esimerkiksi, jos G_1 ja G_2 ovat ryhmiä, niin $\prod_{\alpha \in \{1,2\}} G_\alpha = G_1 \times G_2$ ja laskutoimitus on

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$$

kaikille $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$.

Seuraus 8.13. *Olkoot G_1 ja G_2 ryhmiä. Niiden tulo $G_1 \times G_2$ varustettuna komponenteittaisella laskutoimituksella on ryhmä. Jos e_1 ja e_2 ovat ryhmien G_1 ja G_2 neutraalialkiot, niin (e_1, e_2) on neutraalialkio joukossa $G_1 \times G_2$. Alkion $(g_1, g_2) \in G_1 \times G_2$ käänteisalkio on (g_1^{-1}, g_2^{-1}) .* □

Esimerkki 8.14. (a) Komponenteittaisella yhteenlaskulla varustetut joukot $(\mathbb{R}^n, +)$ ja $(\mathbb{Z}^n, +)$ ovat ryhmiä.

(b) Ryhmät $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ ja yleisemmin $\prod_{i=1}^n \mathbb{Z}/q_i\mathbb{Z}$ ovat äärellisiä ryhmiä kaikille $q, r, q_i \in \mathbb{N} - \{0, 1\}$ ja $n \in \mathbb{N} - \{0\}$.

Esimerkki 8.15. Proposition 1.22 nojalla kompleksikonjugointi on ryhmäisomorfismi $\bar{\cdot}: (\mathbb{C}, +) \rightarrow (\mathbb{C}, +)$ ja $\bar{\cdot}: \mathbb{C}^\times \rightarrow \mathbb{C}^\times$. Kompleksilukujen normi on surjektiivinen ryhmähomomorfismi $|\cdot|: \mathbb{C}^\times \rightarrow \mathbb{R}_+$.

Esimerkki 8.16. Neljän alkion ryhmän $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ laskutaulu on

+	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

Laskutaulussa käytetään kongruenssiluokan $k + 2\mathbb{Z}$ merkintänä edustajaa $k \in \mathbb{Z}$.

8.3 Ryhmähomomorfismit

Jos G ja G' ovat ryhmiä, niin homomorfismia^a $\phi: G \rightarrow G'$ on **ryhmähomomorfismi**.

Bijektiivinen ryhmähomomorfismi on **ryhmäisomorfismi**.

Isomorfismi $\alpha: G \rightarrow G$ on ryhmän G **ryhmäautomorfismi**.

Jos on isomorfismi $\phi: G \rightarrow G'$, niin ryhmät G ja G' ovat **isomorfisia**, $G \cong G'$.

^aKatso luku 1.3.

Esimerkki 8.17. Eksponenttikuvaus $\exp: \mathbb{R} \rightarrow \mathbb{R}_+$, $\exp(x) = e^x$, on ryhmähomomorfismi Esimerkin 1.7 nojalla.

Propositio 8.18. (1) Ryhmähomomorfismien yhdistetty kuvaus on ryhmähomomorfismi.

(2) Isomorfismin käänteiskuvaus isomorfismi.

(3) Jos $G \cong G'$ ja $G' \cong G''$, niin $G \cong G''$.

(4) Jos $G_1 \cong H_1$ ja $G_2 \cong H_2$, niin $G_1 \times G_2 \cong H_1 \times H_2$.

Todistus. Kohdat (1)–(3) seuraavat Propositioista 1.8.

(4) Olkoot $\phi_1: G_1 \rightarrow H_1$ ja $\phi_2: G_2 \rightarrow H_2$ isomorfismeja. Määritellään isomorfismien ϕ_1 ja ϕ_2 tulo $\Phi: G_1 \times G_2 \rightarrow H_1 \times H_2$ asettamalla

$$\Phi(g_1, g_2) = (\phi_1(g_1), \phi_2(g_2))$$

kaikille $(g_1, g_2) \in G_1 \times G_2$.

On helppo tarkastaa, että Φ on bijektio ja sen käänteiskuvauksen lauseke on

$$\Phi^{-1}(h_1, h_2) = (\phi_1^{-1}(h_1), \phi_2^{-1}(h_2)).$$

Riittää siis osoittaa, että Φ on homomorfismi. Olkoot $(g_1, g_2), (g'_1, g'_2) \in G_1 \times G_2$. Tällöin

$$\begin{aligned} \Phi((g_1, g_2)(g'_1, g'_2)) &= \Phi(g_1g'_1, g_2g'_2) = (\phi_1(g_1g'_1), \phi_2(g_2g'_2)) \\ &= (\phi_1(g_1)\phi_1(g'_1), \phi_2(g_2)\phi_2(g'_2)) \\ &= \Phi(g_1, g_2) \Phi(g'_1, g'_2). \end{aligned}$$

□

Propositio 8.19. Ryhmähomomorfismi $\phi: G \rightarrow G'$ kuvaa ryhmän G neutraalialkion ryhmän G' neutraalialkioksi ja jokaiselle $g \in G$ pätee $\phi(g^{-1}) = \phi(g)^{-1}$.

Todistus. (1) Olkoon $\phi: G \rightarrow G'$ homomorfismi. Tällöin

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e),$$

mistä väite seuraa supistussäännöllä.

(2) Olkoon $g \in G$. Tällöin

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e) = e',$$

joten Proposition 8.4(3) nojalla $\phi(g^{-1}) = \phi(g)^{-1}$. \square

Esimerkki 8.20. Jos V ja W ovat \mathbb{R} -vektoriavaruuksia, niin kuvaus $L: V \rightarrow W$ on (\mathbb{R} -)lineaarikuvaus, jos se on homomorfismi kommutatiivisesta ryhmästä $(V, +)$ kommutatiiviseen ryhmään $(W, +)$, joka on lisäksi yhteensopiva reaaliluvulla kertomisen kanssa: Kaikille $\lambda \in \mathbb{R}$ ja $v \in V$ pätee $L(\lambda v) = \lambda L(v)$.

Sen todistaminen, että kaikki homomorfismit reaalilukujen additiiviselta ryhmältä itselleen eivät ole \mathbb{R} -lineaarikuvauksia on monimutkaisempaa. G. Hamel [Ham] todisti tämän tuloksen valinta-aksiooman avulla vuonna 1905.

Esimerkki 8.21. Neljän alkion kommutatiiviset ryhmät $\mathbb{Z}/4\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ eivät ole isomorfsia. Jos nimittäin $\phi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ on homomorfismi, niin kaikille $(a + 2\mathbb{Z}, b + 2\mathbb{Z}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ pätee

$$1 + 4\mathbb{Z} = \phi(1 + 2\mathbb{Z}) = \phi(2(a + 2\mathbb{Z}, b + 2\mathbb{Z})) = 2\phi(a + 2\mathbb{Z}, b + 2\mathbb{Z}).$$

Jos ϕ olisi surjektio, niin kaikille $c + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$ pätsi $2(c + 4\mathbb{Z} \in \mathbb{Z}) = 1 + 4\mathbb{Z}$, mutta tämä ei päde, jos $c = \pm 1$.

8.4 Jäännösluokkien multiplikatiiviset ryhmät

Luvun viimeisenä osana tutustumme vielä yhteen tärkeään kommutatiivisten ryhmien luokkaan.⁶ Tässä luvussa tarvittavat lukuteorian määritelmät ja tulokset on esitetty liitteessä A.

Propositio 8.22. Olkoon $q \geq 2$. Tällöin alkiolla $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on käänteisalkio, jos ja vain jos $\text{sy}(a, q) = 1$. Jos p on alkuluku ja $a \not\equiv 0 \pmod{p}$, niin alkiolla $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})$ on käänteisalkio.

Todistus. Jäännösluokalla $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ on käänteisalkio, jos ja vain jos on $b \in \mathbb{Z}$, jolle

$$1 + q\mathbb{Z} = (a + q\mathbb{Z})(b + q\mathbb{Z}) = ab + q\mathbb{Z}.$$

Tämä pätee, jos ja vain jos on $c \in \mathbb{Z}$, jolle $ab = 1 + cq$. Tämä on Bézout'n yhtälön⁷ nojalla yhtäpitävää sen kanssa, että $\text{sy}(a, q) = 1$. \square

⁶Nyt määriteltävä ryhmä on **renkaan $\mathbb{Z}/q\mathbb{Z}$ yksiköiden ryhmä**. Katso luku 5.3.

⁷Propositio A.3

Propositio 8.23. Joukko $\{a + q\mathbb{Z} : \text{syt}(a, q) = 1\}$ on laskutoimituksella varustetun joukon $(\mathbb{Z}/q\mathbb{Z}, \cdot)$ vakaa osajoukko.

Todistus. Olkoot $a, b \in \mathbb{Z}$ siten, että $\text{syt}(a, q) = \text{syt}(b, q) = 1$. Proposition 8.22 nojalla on $\underline{a}, \underline{b} \in \mathbb{Z}$ siten, että $\text{syt}(\underline{a}, q) = \text{syt}(\underline{b}, q) = 1$ ja

$$(a + q\mathbb{Z})(\underline{a} + q\mathbb{Z}) = 1 + q\mathbb{Z} = (b + q\mathbb{Z})(\underline{b} + q\mathbb{Z}).$$

Tällöin

$$(a + q\mathbb{Z})(b + q\mathbb{Z})(\underline{b} + q\mathbb{Z})(\underline{a} + q\mathbb{Z}) = 1 + q\mathbb{Z},$$

joten Proposition 8.22 nojalla joukko $\{a + q\mathbb{Z} : \text{syt}(a, q) = 1\}$ on vakaa. □

Seuraus 8.24. $(\{a + q\mathbb{Z} : \text{syt}(a, q) = 1\}, \cdot)$ on ryhmä.

Todistus. Seuraa Propositioista 2.9 ja 8.23. □

Olkoon $q \in \mathbb{N} - \{0, 1\}$. Laskutoimituksella varustettu joukko

$$(\mathbb{Z}/q\mathbb{Z})^\times = (\{a + q\mathbb{Z} : \text{syt}(a, q) = 1\}, \cdot)$$

on **jäännösluokkien mod q multiplikatiivinen ryhmä.**

Esimerkki 8.25. $(\mathbb{Z}/8\mathbb{Z})^\times = (\{1 + 8\mathbb{Z}, 3 + 8\mathbb{Z}, 5 + 8\mathbb{Z}, 7 + 8\mathbb{Z}\}, \cdot)$. Ryhmän $(\mathbb{Z}/8\mathbb{Z})^\times$ laskutaulu on

\cdot	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

kun merkitsemme kongruenssiluokkaa $k + 8\mathbb{Z}$ edustajallaan $k \in \mathbb{Z}$.

Esimerkki 8.26. Laskutauluja vertailemalla huomaamme, että kuvaus

$$\begin{aligned} 1 + 8\mathbb{Z} &\mapsto (0 + 2\mathbb{Z}, 0 + 2\mathbb{Z}), \\ 3 + 8\mathbb{Z} &\mapsto (1 + 2\mathbb{Z}, 0 + 2\mathbb{Z}), \\ 5 + 8\mathbb{Z} &\mapsto (0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}), \\ 7 + 8\mathbb{Z} &\mapsto (1 + 2\mathbb{Z}, 1 + 2\mathbb{Z}) \end{aligned}$$

on ryhmäisomorfismi ryhmien $(\mathbb{Z}/8\mathbb{Z})^\times$ ja $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ välillä. Ryhmäteorian kannalta voidaan ajatella, että pohjimmiltaan on kyse samasta abstraktista ryhmästä.

Ryhmä K_4 on **Kleinin neliryhmä**,^a jos

$$K_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

^a4-ryhmä

Jatkossa merkintä K_4 tarkoittaa ryhmää, joka on isomorfinen ryhmän $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ kanssa.

Harjoitustehtäviä

8.1. Olkoon $X \neq \emptyset$. Varustetaan potenssijoukko $\mathcal{P}(X)$ laskutoimituksella Δ (symmetrinen erotus), joka määritellään asettamalla kaikille $A, B \in \mathcal{P}(X)$

$$A \Delta B = (A - B) \cup (B - A).$$

Osoita, että $(\mathcal{P}(X), \Delta)$ on ryhmä.

8.2. Olkoon $X = \{1, 2, 3\}$. Muodosta ryhmän $(\mathcal{P}(X), \Delta)$ laskutaulu.

8.3. Olkoon $(G, *)$ ryhmä. Määritellään uusi laskutoimitus \otimes joukossa G asettamalla

$$a \otimes b = b * a$$

kaikille $a, b \in G$. Osoita, että (G, \otimes) on ryhmä.

8.4. Osoita, että $\text{SL}_n(\mathbb{Z})$ varustettuna matriisien kertolaskulla on ryhmä.⁸

8.5. Todista Propositio 8.6.

8.6. Todista Lemma 8.7.

8.7. Varustetaan joukko $A = \{a, b, c, d, e\}$ laskutoimituksella $*$, jonka laskutaulu on

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	c	e	d	b
b	b	d	c	a	e
c	c	e	d	b	a
d	d	b	a	e	c

Pätevätkö supistussäännöt laskutoimituksella varustetussa joukossa $(A, *)$? Onko $(A, *)$ ryhmä?

8.8. Monellako eri tavalla voit täydentää taulukon

$*$	e	a	b
e	e	a	b
a	a		
b	b		

niin, että tuloksena on ryhmän laskutaulu? Mitä voit päätellä tästä havainnosta?

8.9. Määritellään reaalilukujen joukossa \mathbb{R} laskutoimitus $*$ asettamalla

$$x * y = \sqrt[3]{x^3 + y^3}.$$

Osoita, että $(\mathbb{R}, *)$ on ryhmä, joka on isomorfinen ryhmän $(\mathbb{R}, +)$ kanssa.

8.10. Olkoon $T: \text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z})$, $T(B) = {}^t B$, kuvaus, joka liittää matriisiin B sen transpoosin. Olkoon $\text{inv}: \text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z})$ kuvaus $\text{inv}(B) = B^{-1}$. Mitkä kuvauksista T , inv , $T \circ \text{inv}$ ja $\text{inv} \circ T$ ovat homomorfismeja?⁹

8.11. Minkä kurssilla käsitellyn ryhmän kanssa ryhmä $(\mathbb{Z}/12\mathbb{Z})^\times$ on isomorfinen?

⁸Kertaa lineaarialgebraa! Cramerin sääntö/kofaktorimatriisi.

⁹Kertaa lineaarialgebraa!

Luku 9

Aliryhmät

Tässä luvussa tarkastelemme jonkin ryhmän G osajoukkoja, jotka ovat itsekin ryhmiä ryhmän G laskutoimituksella. Näemme esimerkkejä siitä, miten nämä aliryhmät esiintyvät luonnollisella tavalla muun muassa homomorfismien ytiminä ja tarkastelemme ryhmän osajoukkojen virittämiä aliryhmiä.

9.1 Aliryhmät

Olkoon G ryhmä. Olkoon $B \subset G$, $B \neq \emptyset$, vakaa osajoukko.^a Jos induoidulla laskutoimituksella varustettu joukko B on ryhmä, niin se on ryhmän G **aliryhmä**. Jos $H \subset G$ on ryhmän G aliryhmä, käytämme merkintää $H \leq G$.

Jos aliryhmä H on ryhmän G aito osajoukko, se on ryhmän G **aito aliryhmä**, jolloin käytämme merkintää $H < G$.

^aKatso luku 1.2.

Merkinnät $H \leq G$ ja $H' < G$ sisältävät tietojen $H, H' \subset G$ ja $H' \neq G$ lisäksi siis sen, että H ja H' ovat ryhmiä, joiden laskutoimitus on ryhmän G laskutoimituksen indusoima.

Esimerkki 9.1. (a) Olkoon $a \in \mathbb{Z}$. Tällöin $a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$ on kokonaislukujen ryhmän \mathbb{Z} aliryhmä.

(b) Positiivisten reaalilukujen multiplikatiivinen ryhmä $\mathbb{R}_+ = (]0, \infty[, \cdot)$ on ryhmän \mathbb{R}^\times aito aliryhmä.

Lemma 9.2. *Olkoon G ryhmä. Jokaisen aliryhmän $H \leq G$ neutraalialkio on ryhmän G neutraalialkio.*

Todistus. Jos joillekin $a, b \in H \leq G$ pätee $ab = b$, niin ryhmän G supistussäännön nojalla a on ryhmän G neutraalialkio. \square

Kaikki ryhmän vakaat osajoukot eivät ole ryhmiä, esimerkiksi ryhmän \mathbb{Z} vakaa osajoukko \mathbb{N} ei ole ryhmä. Seuraava tulos antaa keinon tarkastaa, onko jokin ryhmän osajoukko aliryhmä:

Propositio 9.3 (Aliryhmätesti). *Ryhmän G osajoukko $H \neq \emptyset$ on aliryhmä, jos*

- (1) kaikilla $x, y \in H$ pätee $xy^{-1} \in H$, tai
- (2) kaikilla $x, y \in H$ pätee $xy \in H$ ja $y^{-1} \in H$.

Todistus. Olkoon $e \in G$ neutraalialkio. Tarkastellaan ehtoa (1): Olkoon $h \in H$. Oletuksen mukaan $hh^{-1} \in H$, joten $e \in H$. Samoin $y^{-1} = ey^{-1} \in H$ kaikilla $y \in H$. Kaikki on siis kunnossa, jos H on vakaa osajoukko. Edellisen nojalla kaikille $x, y \in H$ pätee $xy = x(y^{-1})^{-1} \in H$, joten H on vakaa.

Ehdosta (2) seuraa ehto (1), joten väite seuraa kohdasta (1). \square

Esimerkki 9.4. (a) Jokaisella ryhmällä on aliryhmiä: ryhmä itse ja neutraalialkion muodostama yhden alkion ryhmä.

(b) $(\{0\}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.

(c) $\{1\} < \{-1, 1\} < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$.

(d) Neliömatriiseista koostuville ryhmille pätee muun muassa

$$\{I_n\} < \{-I_n, I_n\} < \mathrm{GL}_n(\mathbb{Q}) < \mathrm{GL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{C})$$

kaikilla $n \geq 2$ ja

$$\{I_n\} < \{-I_n, I_n\} < \mathrm{SL}_n(\mathbb{Z}) < \mathrm{SL}_n(\mathbb{Q}) < \mathrm{SL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{C}),$$

kun n on parillinen.¹

Esimerkki 9.5. Määritelmän mukaan reaalisen vektoriavaruuden V aliavaruus on osajoukko $H \subset V$, joka on vakaa vektoriavaruuden V yhteenlaskun ja reaaliluvulla kertomisen suhteen ja on näillä operaatioilla varustettuna reaalinen vektoriavaruus. Erityisesti $(H, +)$ on additiivisen ryhmän $(V, +)$ aliryhmä.

Kaikki additiivisen ryhmän $(V, +)$ aliryhmät eivät ole \mathbb{R} -vektoriavaruuden V vektoriavaruuksia. Esimerkiksi \mathbb{R} -vektoriavaruudella \mathbb{R} on vain kaksi aliavaruutta $\{0\}$ ja \mathbb{R} mutta reaalilukujen additiivisella ryhmällä on paljon enemmän aliryhmiä: Esimerkiksi joukot

$$\alpha\mathbb{Z} = \{\alpha k : k \in \mathbb{Z}\} \subset \mathbb{R}$$

ja

$$\alpha\mathbb{Q} = \{\alpha q : q \in \mathbb{Q}\} \subset \mathbb{R}$$

ovat ryhmän $(\mathbb{R}, +)$ vakaita osajoukkoja kaikilla $\alpha \in \mathbb{R}$ ja on helppo tarkastaa, että

$$(\alpha\mathbb{Z}, +) < (\alpha\mathbb{Q}, +) < (\mathbb{R}, +)$$

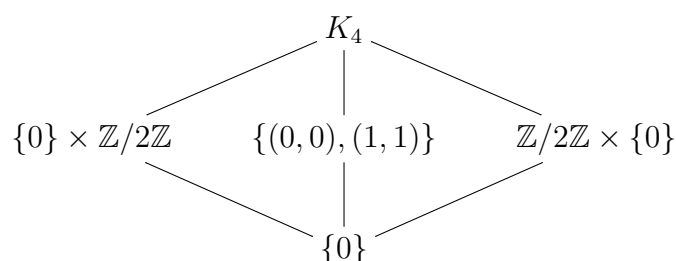
kaikilla $\alpha \in \mathbb{R} - \{0\}$.

Monissa tapauksissa ryhmän rakennetta voi havainnollistaa aliryhmäkaaviolla.

¹Huomaa, että $\det(-I_3) = -1$.

Aliryhmäkaaviossa tarkasteltavan ryhmän aliryhmät asetellaan päällekkäisille tasoille kertaluvun mukaan siten, että kertaluvultaan suuremmat ryhmät ovat ylemmillä tasoilla. Aliryhmä H yhdistetään janalla ylemmällä tasolla olevan aliryhmän K kanssa, jos $H < K$ eikä ole aliryhmää L , jolle pätee $H < L < K$.

Esimerkki 9.6. Olkoon $H \leq (\mathbb{Z}/2\mathbb{Z})^2 = K_4$. Jos $(1 + 2\mathbb{Z}, 0 + 2\mathbb{Z}), (0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}) \in H$, niin $(0 + 2\mathbb{Z}, 0 + 2\mathbb{Z}), (1 + 2\mathbb{Z}, 1 + 2\mathbb{Z}) \in H$, joten $H = K_4$. Vastaavasti nähdään, että ehdoista $(1 + 2\mathbb{Z}, 0 + 2\mathbb{Z}), (1 + 2\mathbb{Z}, 1 + 2\mathbb{Z}) \in H$ ja $(0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}), (1 + 2\mathbb{Z}, 1 + 2\mathbb{Z}) \in H$ seuraa $H = K_4$. Siis ryhmällä K_4 ei ole kolmen alkion aliryhmiä, joten Kleinin 4-ryhmän $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ aliryhmäkaavio on



Tarkastelemme aliryhmäkaavion muodostamista uudelleen luvussa 11.2, jossa todistettava Lagrangen lause² sulkee joitain äärellisen ryhmän aliryhmän kertalukuja pois. Lagrangen lauseen nojalla Esimerkissä 9.6 tarkastellulla Kleinin neliryhmällä ei ole kolmen alkion aliryhmiä. Koska tämä tulos ei vielä ole käytettävissä, tarkastelimme nyt kaikki mahdollisuudet erikseen.

9.2 Homomorfismin ydin

Olkoot G ja G' ryhmiä ja olkoon e' ryhmän G' neutraalialkio. Ryhmähomomorfismin $\phi: G \rightarrow G'$ **ydin** on $\ker \phi = \phi^{-1}(e')$ ja sen **kuva** on $\text{Im } \phi = \phi(G)$.

Propositio 9.7. *Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Tällöin*

- (1) $\phi(H) \leq G'$ kaikilla $H \leq G$. Erityisesti $\text{Im } \phi \leq G'$.
- (2) $\phi^{-1}(H') \leq G$ kaikilla $H' \leq G'$. Erityisesti $\ker \phi \leq G$.

Todistus. (1) Koska H on ryhmä, se sisältää ainakin yhden alkion, joten $\phi(H)$ ei ole tyhjä joukko. Olkoot $\phi(g), \phi(h) \in \phi(H)$. Proposition 8.19 nojalla

$$\phi(g)(\phi(h))^{-1} = \phi(g)\phi(h^{-1}) = \phi(gh^{-1}) \in \phi(H),$$

koska $gh^{-1} \in H$. Siis $\phi(H) \leq G'$ Proposition 9.3(1) nojalla.

(2) Harjoitustehtävä 9.7. □

Esimerkki 9.8. (a) Tekijähomomorfismin $\pi_q: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/q\mathbb{Z}, +)$, $\pi_q(k) = k + q\mathbb{Z}$, ydin on $q\mathbb{Z}$.

(b) Lineaarialgebrassa osoitettiin, että kaikille neliömatriiseille $A, B \in M_n(\mathbb{R})$ pätee

$$\det(AB) = \det A \det B.$$

²Lause 11.10

Kun rajoitetaan determinantti nollajoukkonsa komplementtiin saadaan siis ryhmähomomorfismi $\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$. Determinantin ydin on $SL_n(\mathbb{R})$. Determinantti määritellään samalla lausekkeella myös kompleksikertoimisille neliömatriiseille, jolloin saadaan ryhmähomomorfismi $\det: GL_n(\mathbb{C}) \rightarrow \mathbb{C}^\times$, jonka ydin on $SL_n(\mathbb{C})$.

Tarkastelemme ydintä ja kuvaa lähemmin luvussa 12. Seuraava ytimen ominaisuus on hyvä todeta jo tässä vaiheessa:

Propositio 9.9. *Ryhmähomomorfismi on injektio, jos ja vain jos sen ydin on neutraali-alkion muodostama ryhmä.*

Todistus. Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Aiemmin osoitettiin, että ryhmän G neutraali-alkio e kuvautuu ryhmän G' neutraali-alkioksi e' , joten jos ϕ on injektio, sen ydin on $\{e\}$.

Oletetaan, että $\ker \phi = \{e\}$. Olkoot $x, y \in G$ siten, että $\phi(x) = \phi(y)$. Tällöin

$$\phi(xy^{-1}) = \phi(x)(\phi(y))^{-1} = e',$$

joten $xy^{-1} = e$ eli $x = y$. □

Proposition 9.9 mukaan ryhmähomomorfismin injektiiivisyyden toteamiseksi riittää tarkastella neutraali-alkion alkukuvaa.

9.3 Osajoukon virittämä aliryhmä

Propositio 9.10. *Olkoon G ryhmä, olkoon $I \neq \emptyset$ jokin indeksijoukko ja olkoot $H_i \leq G$ kaikilla $i \in I$. Tällöin*

$$\bigcap_{i \in I} H_i \leq G.$$

Todistus. Harjoitustehtävä 9.8. □

Seuraus 9.11. *Olkoon G ryhmä, olkoot $H_1, H_2 \leq G$. Tällöin $H_1 \cap H_2 \leq G$.*

Todistus. Väite on Proposition 9.10 erikoistapaus indeksijoukolla $I = \{1, 2\}$. □

Olkoon G ryhmä ja olkoon $B \subset G$, $B \neq \emptyset$. Joukon B **virittämä aliryhmä** $\langle B \rangle$ on

$$\langle B \rangle = \bigcap \{H \leq G : B \subset H\} \leq G.$$

Joukko B on aliryhmän $\langle B \rangle$ **virittäjäjoukko** ja joukon B alkioit ovat ryhmän $\langle B \rangle$ **virittäjiä**. Jos $\langle B \rangle = G$, niin joukko B **virittää** ryhmän G .

Proposition 9.10 nojalla joukon B virittämä aliryhmä on pienin joukon B sisältävä aliryhmä. Erityisesti, jos $H \leq G$, niin $\langle H \rangle = H$.

Edellä annettu määritelmä on abstrakti tapa ajatella osajoukon virittämää aliryhmää. Usein on hyödyllistä tietää, miten ryhmä $\langle B \rangle$ voidaan esittää konkreettisesti virittäjiensä avulla:

Propositio 9.12. *Olkoon G ryhmä ja olkoon $e \in G$ neutraalialkio. Olkoon $B \subset G$, $B \neq \emptyset$. Olkoon $B^{-1} = \{b^{-1} : b \in B\}$. Joukon B virittämä aliryhmä on*

$$\begin{aligned} & \{b_1^{\pm 1} b_2^{\pm 1} \cdots b_k^{\pm 1} : b_1, b_2, \dots, b_k \in B, k \in \mathbb{N} - \{0\}\} \\ & = \{a_1 a_2 \cdots a_k : a_1, a_2, \dots, a_k \in B \cup B^{-1}, k \in \mathbb{N} - \{0\}\}. \end{aligned} \quad (9.1)$$

Todistus. Lausekkeen (9.1) antama osajoukko \tilde{B} on ryhmän G aliryhmä Propositioiden 8.4(4) ja 9.3 nojalla. Erityisesti \tilde{B} on ryhmä, joka sisältää joukon B , joten $\langle B \rangle \leq \tilde{B}$.

Toisaalta $\langle B \rangle$ on ryhmän G aliryhmä, joten erityisesti se on vakaa osajoukko. Koska $B \subset \langle B \rangle$, niin jokaisen alkion $b \in B$ käänteisalkio b^{-1} kuuluu ryhmään $\langle B \rangle$. Induktiolla on helppo nähdä, että vakauudesta seuraa, että $\langle B \rangle$ sisältää kaikki muotoa $b_1^{\pm 1} b_2^{\pm 1} \cdots b_k^{\pm 1}$ olevat alkioita. Siis $\tilde{B} \leq \langle B \rangle$. \square

Propositio 9.12 nojalla ryhmän G osajoukon B virittämä aliryhmä koostuu kaikista niistä ryhmän G alkioista, jotka voidaan esittää sanoina joukon B alkioista ja niiden käänteisalkioista.

Esimerkki 9.13. (a) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ ja kaikilla $q \in \mathbb{Z} - \{-1, 1\}$ pätee $\langle q \rangle < \mathbb{Z}$. Toisaalta $\mathbb{Z} = \langle 2, 3 \rangle = \langle 6, 10, 15 \rangle$, koska $1 = 3 - 2 = 6 + 10 - 15$, mutta aliryhmät $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 6, 10 \rangle = \langle 2 \rangle$, $\langle 6, 15 \rangle = \langle 3 \rangle$ ja $\langle 10, 15 \rangle = \langle 5 \rangle$ ovat ryhmän $(\mathbb{Z}, +)$ aitoja aliryhmiä.

(b) Kokeilemalla kaikki tapaukset on helppo nähdä, että jokainen nollasta poikkeava alkio virittää ryhmän $\mathbb{Z}/5\mathbb{Z}$:

$$\mathbb{Z}/5\mathbb{Z} = \langle 1 + 5\mathbb{Z} \rangle = \langle 2 + 5\mathbb{Z} \rangle = \langle 3 + 5\mathbb{Z} \rangle = \langle 4 + 5\mathbb{Z} \rangle.$$

Toisaalta $\mathbb{Z}/4\mathbb{Z} = \langle 1 + 4\mathbb{Z} \rangle = \langle 3 + 4\mathbb{Z} \rangle$ mutta $\langle 2 + 4\mathbb{Z} \rangle = \{0 + 4\mathbb{Z}, 2 + 4\mathbb{Z}\} < \mathbb{Z}/4\mathbb{Z}$.

(c) Jos G on ryhmä, $B \subset G$ ja $b \in B$, niin ryhmän G neutraalialkio e voidaan esittää äärettömän monen sanan avulla $e = bb^{-1} = b^{-1}b = bbb^{-1}b^{-1} = \dots$. Tästä seuraa, että jokainen aliryhmän $\langle B \rangle$ alkio voidaan esittää äärettömän monella eri tavalla sanana joukon $B \cup B^{-1}$ alkioista.

Monissa ryhmissä monet muutkin eri sanat vastaavat samaa alkioita: Jos G on äärellinen ryhmä, virittäjäjoukosta muodostettuja sanoja on äärettömän monta ja niiden avulla voidaan kuitenkin esittää vain äärellisen monta alkioita. Toisaalta, jos H on kommutatiivinen ryhmä ja $B \subset H$, niin $ab = ba$ kaikille $a, b \in B$.

Seuraava tulos yleistää Esimerkissä 9.13(b) tehdyn havainnon.

Propositio 9.14. *Olkoon $q \geq 2$. Tällöin $\mathbb{Z}/q\mathbb{Z} = \langle a + q\mathbb{Z} \rangle$, jos ja vain jos $\text{syt}(a, q) = 1$.*

Todistus. Jos $\text{syt}(a, q) = s \geq 2$, niin $\frac{a}{s}, \frac{q}{s} \in \mathbb{Z}$ ja $\frac{a}{s} a = q \frac{a}{s} \in q\mathbb{Z}$, joten ryhmässä $\langle a + q\mathbb{Z} \rangle$ on korkeintaan $\frac{a}{s} < q$ alkioita. Oletetaan sitten, että $\text{syt}(a, q) = 1$. Kaikki ryhmän $\mathbb{Z}/q\mathbb{Z}$ alkioita ovat alkion $1 + q\mathbb{Z}$ monikertoja, joten $a + q\mathbb{Z}$ on virittäjä, jos $1 + q\mathbb{Z} \in \langle a + q\mathbb{Z} \rangle$. Bézout'n yhtälön³ nojalla on $x, y \in \mathbb{Z}$ siten, että $ax + qy = 1$ mutta tähän tarkoittaa, että $x(a + q\mathbb{Z}) = 1 + q\mathbb{Z}$. \square

Seuraava tulos osoittaa, että ryhmässä G määritelty ryhmähomomorfismi määräytyy yksikäsitteisesti, jos sen arvot tunnetaan virittäjäjoukossa.

³Propositio A.3

Propositio 9.15. Olkoon $G = \langle S \rangle$ ryhmä. Olkoot $\phi, \psi: G \rightarrow H$ ryhmähomomorfismeja, joille pätee $\phi|_S = \psi|_S$. Tällöin $\phi = \psi$.

Todistus. Harjoitustehtävä 9.9. □

9.4 Syklinen ryhmä

Olkoon G multiplikatiivinen ryhmä ja olkoon H additiivinen ryhmä. Aliryhmät

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} \leq G$$

ja

$$\langle b \rangle = \{nb : n \in \mathbb{Z}\} \leq H$$

ovat alkioden $a \in G$ ja $b \in H$ virittämät sykliset aliryhmät.

Ryhmä Z on **syklinen ryhmä**, jos on $a \in Z$ siten, että $Z = \langle a \rangle$.

Esimerkki 9.16. (a) Edellä käsitellyistä esimerkeistä muun muassa ryhmät $\mathbb{Z} = \langle 1 \rangle$ ja $\mathbb{Z}/q\mathbb{Z} = \langle 1 + q\mathbb{Z} \rangle$, $q \geq 2$, ovat syklisiä.

(b) Ryhmän $(\mathbb{R}^2, +)$ alkioit $(0, 1)$ ja $(1, 0)$ virittävät aliryhmän

$$\langle (0, 1), (1, 0) \rangle = (\mathbb{Z}^2, +) < (\mathbb{R}^2, +).$$

$(\mathbb{Z}^2, +)$ ei ole syklinen ryhmä: Jos $a, b \in \mathbb{Z} - \{0\}$, niin $(-a, b) \notin \langle (a, b) \rangle$. Lisäksi alkioden $(a, 0)$ ja $(0, a)$ virittämät sykliset ryhmät sisältyvät ryhmän $(\mathbb{Z}^2, +)$ aitoihin aliryhmiin $\mathbb{Z} \times \{0\}$ ja $\{0\} \times \mathbb{Z}$, joten myöskään tätä muotoa olevat alkioit eivät voi yksinään virittää ryhmää $(\mathbb{Z}^2, +)$.

(c) Kleinin neliryhmä K_4 ei ole syklinen, koska jokaisen neutraalialkiosta poikkeavan alkion virittämä syklinen ryhmä on isomorfinen ryhmän $\mathbb{Z}/2\mathbb{Z}$ kanssa.

Ryhmän G alkion g **kertaluku** $\text{ord } g$ on sen virittämän syklisen aliryhmän kertaluku, $\text{ord } g = \#\langle g \rangle$.

Lemma 9.17. Olkoon G ryhmä ja olkoon e ryhmän G neutraalialkio. Jos jollain $k \in \mathbb{N} - \{0\}$ pätee $g^k = e$, niin

$$\text{ord } g = \min\{k \geq 1 : g^k = e\}.$$

Lisäksi

$$\langle g \rangle = \{e, g, g^2, \dots, g^{\text{ord } g - 1}\}.$$

Todistus. Harjoitustehtävä 9.13. □

Esimerkki 9.18. (a) Ryhmän K_4 kertaluku on 4 ja sen jokaisen neutraalialkiosta poikkeavan alkion kertaluku on 2.

(b) Ryhmän $\mathbb{Z}/4\mathbb{Z}$ kertaluku on 4 ja sen alkioden $1 + 4\mathbb{Z}$ ja $3 + 4\mathbb{Z}$ kertaluku on 4. Tämä on helppo tarkastaa vaikka alkioille $3 + 4\mathbb{Z}$:

$$2(3 + 4\mathbb{Z}) = (3 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4\mathbb{Z},$$

$$3(3 + 4\mathbb{Z}) = (2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$$

ja

$$4(3 + 4\mathbb{Z}) = (1 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = (4 + 4\mathbb{Z}) = 0.$$

Kokonaislukujen additiivisella ryhmällä on sykliset aliryhmät

$$n\mathbb{Z} = \langle n \rangle = \{kn : k \in \mathbb{Z}\},$$

$n \in \mathbb{N}$. Itse asiassa ryhmällä $(\mathbb{Z}, +)$ ei ole mitään muita aliryhmiä:

Propositio 9.19. *Kokonaislukujen ryhmän \mathbb{Z} kaikki aliryhmät ovat syklisiä.*

Todistus. Huomataan ensin, että $\{0\} = 0\mathbb{Z}$ ja $\mathbb{Z} = 1\mathbb{Z}$. Olkoon $H < \mathbb{Z}$, $H \neq \{0\}$ jokin aliryhmä. Tällöin $H \cap (\mathbb{N} - \{0\})$ ei ole tyhjä ja tässä joukossa on pienin positiivinen kokonaisluku $q \in H$. Erityisesti $q\mathbb{Z} < H$.

Osoitamme, että $H = q\mathbb{Z}$. Jos on $m \in H - q\mathbb{Z}$, niin kokonaislukujen jakoyhtälön⁴ nojalla $m = aq + b$ joillakin $a, b \in \mathbb{Z}$ siten, että $1 \leq b < q$. Nyt $b \in H$, joten q ei olekaan pienin positiivinen kokonaisluku ryhmässä H , mikä on ristiriita. Siis $H = q\mathbb{Z}$. \square

Lause 9.20. (1) *Syklisen ryhmän, jossa on vähintään kaksi alkioita, on isomorfinen joko ryhmän \mathbb{Z} tai jonkin ryhmän $\mathbb{Z}/q\mathbb{Z}$, $q \geq 2$ kanssa.*

(2) *Syklisen ryhmän kuva ryhmähomomorfismissa on syklinen.*

(3) *Jokainen syklisen ryhmän aliryhmä on syklinen.*

Todistus. (1) Olkoon $C = \langle g \rangle$ syklinen ryhmä ja olkoon $\phi: \mathbb{Z} \rightarrow C$, $\phi(n) = g^n$. Lemman 1.23 nojalla ϕ on homomorfismi ja ryhmän C määritelmän nojalla se on surjektio. Jos ϕ on injektio, se on isomorfismi.

Jos ϕ ei ole injektio, niin Propositoiden 9.7, 9.9 ja 9.19 nojalla $\ker \phi = q\mathbb{Z}$ jollain $q \geq 2$. Olkoon $\psi: (\mathbb{Z}/q\mathbb{Z}, +) \rightarrow C$,

$$\psi(k + q\mathbb{Z}) = \phi(k) = g^k.$$

Kuvaus ψ on hyvin määritelty: jos $k \equiv k' \pmod{q}$, niin $k - k' \in q\mathbb{Z} = \ker \phi$, joten $g^k = g^{k'} g^{k-k'} = g^{k'}$. Kuvaus ψ on homomorfismi:

$$\begin{aligned} \psi(n + q\mathbb{Z}) \psi(m + q\mathbb{Z}) &= g^n g^m = g^{n+m} = \psi((n+m) + q\mathbb{Z}) \\ &= \psi((n + q\mathbb{Z}) + (m + q\mathbb{Z})). \end{aligned}$$

Homomorfismi ψ on surjektio, koska ϕ on surjektio. Proposition 9.9 nojalla injektiiivisuuden todistamiseen riittää osoittaa, että $\ker \psi = \{0\}$. Oletetaan, että $\psi(k + q\mathbb{Z}) = e \in G$. Tällöin $\phi(k) = e$, joten $k \in q\mathbb{Z}$ ja $k + q\mathbb{Z} = q\mathbb{Z} = 0$.

(2) Harjoitustehtävä 9.19.

(3) Väite todistettiin sykliselle ryhmälle \mathbb{Z} Propositiossa 9.19. Olkoon $C = \langle g \rangle$ syklinen ryhmä ja olkoon $H < C$. Olkoon $\phi: \mathbb{Z} \rightarrow C$ (surjektiiivinen) homomorfismi $\phi(n) = g^n$. Tällöin Proposition 9.7 nojalla $\phi^{-1}(H) \leq \mathbb{Z}$, joten Proposition 9.19 nojalla $\phi^{-1}(H) = N\mathbb{Z}$ jollain $N \in \mathbb{Z}$. Erityisesti $\phi^{-1}(H)$ on syklinen ryhmä. Koska $H = \phi(\phi^{-1}(H))$, väite seuraa kohdasta (2). \square

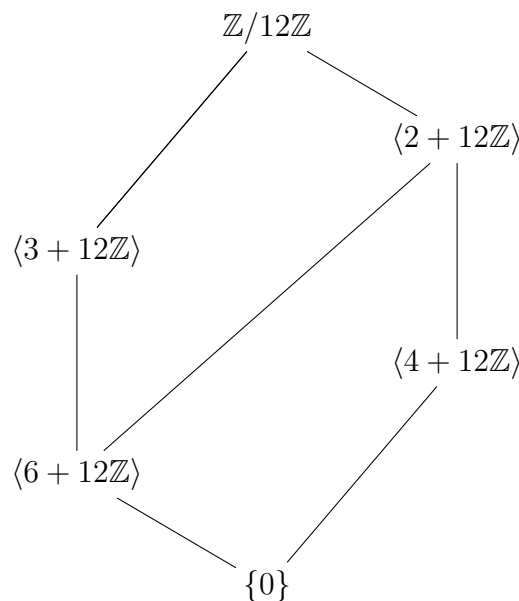
⁴Propositio A.1

Esimerkki 9.21. Ryhmät \mathbb{Q} ja \mathbb{R} eivät ole syklisiä. Reaaliluvuille tämä on selvää, koska syklinen ryhmä on Lauseen 9.20 seurauksena aina numeroituva. Rationaalilukujen tapaus käsitellään harjoitustehtävässä 9.16.

Koska Lauseen 9.20 mukaan kaikki keskenään yhtä mahtavat sykliset ryhmät ovat isomorfisia keskenään, voimme puhua abstraktista n alkion syklisestä ryhmästä C_n ja äärettömästä syklisestä ryhmästä C_∞ .^a

^aToisinaan syklisille ryhmille käytetään merkintöjä Z_n ja Z_∞ .

Esimerkki 9.22. Ryhmän $\mathbb{Z}/12\mathbb{Z}$ aliryhmäkaavio on



9.5 Ryhmien sisäinen suora tulo

Olkoon G ryhmä ja olkoot $S, T \leq G$. Tällöin

$$ST = \{st : s \in S, t \in T\}.$$

Proposition 9.12 nojalla

$$S \cup T \subset ST = \{st : s \in S, t \in T\} \subset \langle S \cup T \rangle.$$

Siis, jos ST on ryhmä, niin $ST = \langle S \cup T \rangle$. Seuraava esimerkki osoittaa, että ST ei välttämättä ole ryhmä. Myöhemmin todistettava Propositio 12.22 antaa riittävän ehdon sille, että $ST = \langle S \cup T \rangle$.

Esimerkki 9.23. Olkoot

$$U = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle, \quad L = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \leq \mathrm{SL}_2(\mathbb{R}).$$

Tällöin

$$UL = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} = \begin{pmatrix} 1 + mn & m \\ n & 1 \end{pmatrix} : m, n \in \mathbb{Z} \right\}.$$

Jos $m, n \neq 0$, niin

$$\begin{pmatrix} 1 + mn & m \\ n & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -m \\ -n & 1 + mn \end{pmatrix}$$

ei ole joukossa UL , joten UL ei ole ryhmän $SL_2(\mathbb{R})$ aliryhmä. Vastaavalla tavalla nähdään, että LU ei ole ryhmä.

Olkoon G ryhmä, jonka neutraalialkio on e , ja olkoot $H, J \leq G$ aliryhmiä. Jos $HJ = G$, $H \cap J = \{e\}$ ja $hj = jh$ kaikille $h \in H$ ja $j \in J$. Tällöin G on aliryhmien H ja J **sisäinen suora tulo**.

Sisäisen suoran tulon määritelmässä edellytetään, että aliryhmien H ja J alkioille pätee $hj = jh$ kaikille $h \in H$ ja $j \in J$. Tämä ehto on usein kätevä ilmaista sanallisesti, seuraava määritelmä antaa sanastoa:

Olkoon $(A, *)$ laskutoimituksella varustettu joukko. Jos $a, h \in A$ ja $g * h = h * g$, niin g ja h **kommutoivat**.

Propositio 9.24. *Olkoon G aliryhmien H ja J sisäinen suora tulo. Tällöin $G \cong H \times J$.*

Todistus. Harjoitustehtävä 9.25. □

Esimerkki 9.25. Esimerkissä 8.25 tarkasteltu ryhmä $(\mathbb{Z}/8\mathbb{Z})^\times$ on aliryhmiensä $\langle 3 + 8\mathbb{Z} \rangle$ ja $\langle 5 + 8\mathbb{Z} \rangle$ sisäinen suora tulo:

$$(3 + 8\mathbb{Z})^2 = (5 + 8\mathbb{Z})^2 = 1 + 8\mathbb{Z} \quad \text{ja} \quad (3 + 8\mathbb{Z})(5 + 8\mathbb{Z}) = 7 + 8\mathbb{Z},$$

joten $\langle 3 + 8\mathbb{Z} \rangle \langle 5 + 8\mathbb{Z} \rangle = (\mathbb{Z}/8\mathbb{Z})^\times$.⁵ Lisäksi $\langle 3 + 8\mathbb{Z} \rangle \cap \langle 5 + 8\mathbb{Z} \rangle = \{1 + 8\mathbb{Z}\}$ ja sisäisen suoran tulon kommutoisuus ehto pätee, koska $(\mathbb{Z}/8\mathbb{Z})^\times$ on kommutatiivinen.

Propositio 9.24 nojalla $(\mathbb{Z}/8\mathbb{Z})^\times$ on siis isomorfinen suoran tulon $\langle 3 + 8\mathbb{Z} \rangle \times \langle 5 + 8\mathbb{Z} \rangle$ kanssa. Huomaa, että aliryhmät $\langle 3 + 8\mathbb{Z} \rangle$ ja $\langle 5 + 8\mathbb{Z} \rangle$ ovat kahden alkion sykliisiä ryhmiä Lemman 9.17 nojalla. Siis Proposition 8.18(4) nojalla $(\mathbb{Z}/8\mathbb{Z})^\times$ on Kleinin neliryhmä.

9.6 Lineaarialgebran ryhmiä

Matematiikan eri aloilla joukkoihin voidaan liittää erilaisia lisärakenteita kuten vektoriaruusrakenne, sisätulo, laskutoimitus tai etäisyysfunktio. Tällaisten joukkojen permutaatioryhmien osajoukot, jotka säilyttävät valitun rakenteen tai ovat sen kanssa yhteensopivia, ovat usein ryhmiä.

Vektoriaruuden \mathbb{R}^n **yleinen lineaarinen ryhmä** on

$$GL(\mathbb{R}^n) = \{L \in \text{Perm}(\mathbb{R}^n) : L \text{ on lineaarikuvaus}\}.$$

Propositio 9.26. $GL(\mathbb{R}^n) \cong GL_n(\mathbb{R})$.

⁵Suoran tulon määritelmän merkinnöillä $H = \langle 3 + 8\mathbb{Z} \rangle$, $J = \langle 5 + 8\mathbb{Z} \rangle$ ja $G = (\mathbb{Z}/8\mathbb{Z})^\times$ pätee siis $HJ = G$.

Todistus. Olkoon $\text{Mat}: \text{GL}(\mathbb{R}^n) \rightarrow \text{GL}_n(\mathbb{R})$ kuvaus, joka liittää lineaarikuvaukseen $L \in \text{GL}(\mathbb{R}^n)$ sen matriisin standardikannan e_1, e_2, \dots, e_n suhteen:

$$\text{Mat}(L)_{ij} = (e_i | Le_j)$$

kaikille $1 \leq i, j \leq n$. Lineaarialgebran kurssilla osoitetaan, että kaikille $L_1, L_2 \in \text{GL}(\mathbb{R}^n)$ pätee

$$\text{Mat}(L_1 L_2) = \text{Mat}(L_1) \text{Mat}(L_2).$$

Lisäksi on helppo tarkastaa, että jokainen matriisi $A \in \text{GL}_n(\mathbb{R})$ määrää lineaarikuvauksen $L_A \in \text{GL}(\mathbb{R}^n)$ asettamalla $L_A(x) = Ax$ kaikille $x \in \mathbb{R}^n$ ja että $\text{Mat}(L_A) = A$ kaikille $A \in \text{GL}_n(\mathbb{R})$. \square

Olkoon G ryhmä ja olkoon $X \neq \emptyset$. Ryhmän G **toiminta joukolla** X on homomorfismi $\rho: G \rightarrow \text{Perm}(X)$.

Jos toiminta on injektio, se on **uskollinen toiminta**.

Esimerkki 9.27. Isomorfismi Mat^{-1} on ryhmän $\text{GL}_n(\mathbb{R})$ uskollinen toiminta joukolla \mathbb{R}^n .

Olkoon $\rho: G \rightarrow \text{Perm}(X)$ ryhmän G toiminta joukolla X . Usein homomorfismi ρ jätetään merkittömättä ja kuvausta $\rho(g): X \rightarrow X$ merkitään alkiolla $g \in G$. Merkintä $g(x)$ tarkoittaa tällaisessa yhteydessä samaa kuin merkintä $(\rho(g))(x)$.

Jatkossa samastamme sujuvasti matriisin ja sen standardikannassa määräämän lineaarikuvauksen.

Bilineaarikuvaus $(\cdot | \cdot): \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$,

$$(x | y) = \sum_{i=1}^n x_i y_i,$$

on **euklidinen sisätulo**.

Funktio $\|\cdot\|: \mathbb{R}^n \rightarrow [0, \infty[$,

$$\|x\| = \sqrt{(x | x)} = \sqrt{\sum_{i=1}^n x_i^2},$$

on **euklidinen normi**.

Kolmikko $(\mathbb{R}^n, (\cdot | \cdot), \|\cdot\|)$ on **euklidinen avaruus** \mathbb{E}^n .

Euklidisen avaruuden \mathbb{E}^n **ortogonaaliryhmä** on

$$\text{O}(n) = \{A \in \text{GL}_n(\mathbb{R}) : {}^t A A = I_n\},$$

missä ${}^t A$ on matriisin A transpoosi. Euklidisen avaruuden \mathbb{E}^n **erityinen ortogonaaliryhmä** on

$$\text{SO}(n) = \{A \in \text{O}(n) : \det A = 1\}.$$

Lemma 9.28. *Kaikille $A \in O(n)$ ja kaikille $x, y \in \mathbb{E}^n$ pätee $(Ax \mid Ay) = (x \mid y)$. Erityisesti kaikille $x \in \mathbb{R}^n$ pätee $\|Ax\| = \|x\|$.*

Todistus. Lineaarialgebran tiedoilla saamme

$$(Ax \mid Ay) = {}^t(Ax)Ay = {}^t x {}^t A A y = {}^t x y = (x \mid y)$$

kaikille $A \in O(n)$ ja kaikille $x, y \in \mathbb{E}^n$. Molemmat väitteet seuraavat tästä. □

Lemma 9.29. $O(n) < GL_n(\mathbb{R})$.

Todistus. Harjoitustehtävä 9.26. □

Yleisen lineaarisen ryhmän aliryhmänä ortogonaaliryhmä $O(n)$ toimii vektoriavaruuksella \mathbb{R}^n lineaarikuvauksilla.

9.7 Lukuteorian ryhmiä

Seuraava pieni havainto antaa ryhmäteoreettisen näkökulman Bézoutin yhtälöön⁶ ja suurimpaan yhteiseen tekijään. Kahden kokonaisluvun suurin yhteinen tekijä määritellään liitteessä A.

Propositio 9.30. *Olkoot $m, n \in \mathbb{Z} - \{0\}$. Jos $\langle m, n \rangle = \langle d \rangle$, niin $d = \pm \text{syt}(m, n)$.*

Todistus. Luku d on lukujen m ja n yhteinen tekijä, koska $m, n \in \langle d \rangle$. Olkoon $e \neq 0$ lukujen m ja n yhteinen tekijä. Koska $d \in \langle m, n \rangle$, on luvut $r, s, m_1, n_1 \in \mathbb{Z}$ siten, että

$$d = rm + sn = r(m_1e) + s(n_1d) = (rm_1 + sn_2)e,$$

joten e jakaa luvun d . Siis d on lukujen m ja n suurin yhteinen tekijä. □

Seuraus 9.31. *Nollasta poikkeavilla kokonaisluvuilla on suurin yhteinen tekijä.*

Todistus. Olkoot $m, n \in \mathbb{Z} - \{0\}$. Proposition 9.19 mukaan kaikki kokonaislukujen additiivisen ryhmän aliryhmät ovat sykliisiä, joten on $d \in \mathbb{N}$ siten, että $\langle d \rangle = \langle m, n \rangle$. Väite seuraa siis Propositioista 9.30. □

Olkoot $a, b \in \mathbb{Z}$. Lukujen a ja b **pienin yhteinen jaettava** on

$$\text{pyj}(a, b) = \min\{c \in \mathbb{N} - \{0\} : a \text{ ja } b \text{ ovat luvun } c \text{ tekijöitä}\}.$$

Seuraava helppo Lemma kuvailee pienimmän yhteisen tekijän ryhmäteoreettisesti.

Lemma 9.32. *Olkoot $a, b \in \mathbb{Z}$. Tällöin*

$$a\mathbb{Z} \cap b\mathbb{Z} = \text{pyj}(a, b)\mathbb{Z}.$$

Todistus. Harjoitustehtävä 9.27. □

⁶Propositio A.3

Harjoitustehtäviä

9.1. Osoita, että

$$\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\} = \{\cos(t) + i \sin(t) : t \in \mathbb{R}\}$$

on ryhmän \mathbb{C}^\times aliryhmä.⁷

9.2. Anna esimerkki surjektiivisestä homomorfismista $f: (\mathbb{R}, +) \rightarrow (\mathbb{S}^1, \cdot)$.⁸

9.3. Olkoon $q \in \mathbb{N} - \{0\}$. Osoita, että joukko

$$J_q = \{w \in \mathbb{C} : w^q = 1\}$$

varustettuna kompleksilukujen kertolaskulla on ryhmän \mathbb{C}^\times aliryhmä.

Kolmeulotteinen **Heisenbergin ryhmä** on joukko

$$H_3 = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{R} \right\}$$

varustettuna matriisien kertolaskulla.

9.4. Osoita, että H_3 on ryhmä.

9.5. Osoita, että ryhmä H_3 ei ole isomorfinen ryhmän $(\mathbb{R}^3, +)$ kanssa.⁹

Ryhmän G **keskus** on

$$Z(G) = \{z \in G : zg = gz \text{ kaikilla } g \in G\}.$$

9.6. Olkoon G ryhmä. Osoita, että $Z(G) \leq G$.

9.7. Todista Propositio 9.7(2).

9.8. Todista Propositio 9.10.

9.9. Todista Propositio 9.15.

9.10. Osoita, että ryhmät $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ovat isomorfisia.¹⁰

9.11. Olkoot $q, r \in \mathbb{N} - \{0, 1\}$ lukuja, joiden suurin yhteinen tekijä on 1. Osoita, että¹¹

$$\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z} \cong \mathbb{Z}/qr\mathbb{Z}.$$

9.12. Osoita, että $(\mathbb{Z}/6\mathbb{Z})^\times$ ja $(\mathbb{Z}/10\mathbb{Z})^\times$ ovat syklisiä ryhmiä.

9.13. Todista Lemma 9.17.

⁷Opiskele tarvittaessa kompleksiluvuista luvusta 1.7, jonka tuloksia voi käyttää.

⁸Joukon \mathbb{S}^1 jälkimmäinen esitysmuoto Harjoitustehtävässä 9.1 saattaa auttaa.

⁹Propositio 1.10

¹⁰Osoita, että $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ on syklinen ryhmä.

¹¹Propositio A.4

9.14. Määritä luvun $\omega = \frac{1+i\sqrt{3}}{2} \in \mathbb{C}^\times$ kertaluku. Mitkä kompleksiluvut muodostavat aliryhmän $\langle \omega \rangle$?

9.15. Olkoon G ryhmä. Oletetaan, että jokaisen alkion $g \in G$, joka ei ole neutraalialkio, kertaluku on 2. Osoita, että G on kommutatiivinen ryhmä.

9.16. Osoita, että rationaalilukujen additiivinen ryhmä ei ole syklinen.¹²

9.17. Olkoon $S \subset \mathbb{Q}$ äärellinen joukko. Osoita, että joukon S virittämä aliryhmä on syklinen ja että se on ryhmän $(\mathbb{Q}, +)$ aito aliryhmä.

9.18. Osoita, että rationaalilukujen multiplikatiivinen ryhmä \mathbb{Q}^\times ei ole syklinen.¹³

9.19. Todista Lause 9.20(2).

9.20. Määritä $\langle 30, 42, 70, 105 \rangle \leq (\mathbb{Z}, +)$.

9.21. Olkoon G ryhmä ja olkoon $H \subset G$ äärellinen vakaa osajoukko, jossa on ainakin yksi alkio.¹⁴ Osoita, että $H \leq G$.

Kommutatiivisen ryhmän G torsioaliryhmä on

$$\text{Tor } G = \{g \in G : \text{ord } g < \infty\}.$$

9.22. Osoita, että $\text{Tor } G$ on kommutatiivisen ryhmän G aliryhmä.

9.23. Määritä $\text{Tor}(\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z}))$.

9.24. Määritä matriisien $A, B, C \in \text{SL}_2(\mathbb{Z})$ kertaluvut, kun

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{ja} \quad C = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Osoita, että joukko

$$\{F \in \text{SL}_2(\mathbb{Z}) : \text{ord } F < \infty\}$$

ei ole ryhmän $\text{SL}_2(\mathbb{Z})$ aliryhmä.

9.25. Todista Propositio 9.24.

9.26. Todista Lemma 9.29.

9.27. Todista Lemma 9.32.

¹²Jos se olisi syklinen, niin

¹³Aritmetiikan peruslause (Lause A.7) auttaa.

¹⁴Miten sykliset ryhmät liittyvät tähän?

Luku 10

Symmetriset ryhmät

Tässä luvussa tarkastelemme äärellisten joukkojen permutaatioryhmiä, joita kutsutaan symmetrisiksi ryhmiksi. Symmetriset ryhmät antavat meille esimerkkejä äärellisistä ryhmistä, jotka eivät ole kommutatiivisia. Niillä on paljon sovelluksia esimerkiksi geometriassa ja kombinatoriikassa.

10.1 Symmetrinen ryhmä S_n

Harjoitustehtävän 10.1 nojalla kaikkien n alkion joukkojen permutaatioryhmät¹ ovat isomorfisia keskenään.

Äärellisen n alkioista koostuvan joukon permutaatioryhmä on **symmetrinen ryhmä** S_n .

Jokaisen n alkioista koostuvan joukon permutaatioryhmää sanotaan ryhmäksi S_n vastaavalla tavalla kuin voidaan puhua abstrakteista syklistä ryhmistä C_n ja C_∞ . Kun todistetaan väitteitä symmetriselle ryhmälle S_n , voidaan todistuksessa tarkastella esimerkiksi joukon $\{1, 2, \dots, n\}$ permutaatioita.

Symmetriset ryhmät ovat tärkeitä matematiikan eri aloilla, esimerkiksi Galois'n teoriassa, joka käsittelee muun muassa polynomien algebrallista ratkeavuutta, samoin ne tulevat vastaan geometriassa tarkasteltaessa esimerkiksi säännöllisten monikulmioiden ja monitahokkaiden symmetriaryhmiä. Tästä saamme hieman esimakua luvussa 13.2.

Propositio 10.1. (1) *Symmetrisen ryhmän S_n kertaluku on $n!$.*

(2) *Jos $n \geq 3$, niin S_n ei ole kommutatiivinen.*

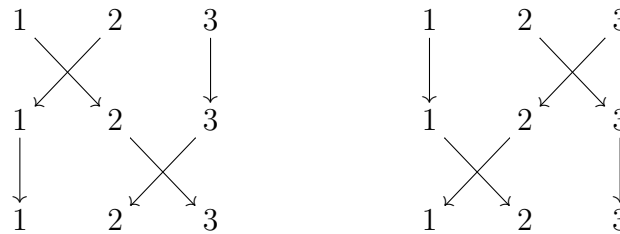
Todistus. (1) Harjoitustehtävä.

(2) Tarkastellaan ensin tapaus $n = 3$. Olkoon $\sigma \in S_3$, $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$ ja olkoon $\tau \in S_3$, $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 2$. Tällöin $\tau \circ \sigma(1) = \tau(2) = 3$ ja $\sigma \circ \tau(1) = \sigma(1) = 2$, joten $\sigma \circ \tau \neq \tau \circ \sigma$.

¹Katso määritelmä Esimerkin 8.11 jälkeen.

Edellä määritellyt permutaatiot on helppo laajentaa n alkion permutaatioiksi määrittelemällä kaikille $n \geq 4$ permutaatiot $\bar{\sigma}, \bar{\tau} \in S_n$, joille $\bar{\sigma}|_{\{1,2,3\}} = \sigma$, $\bar{\tau}|_{\{1,2,3\}} = \tau$, ja $\bar{\sigma}(k) = k = \bar{\tau}(k)$ kaikille $4 \leq k \leq n$. Näille permutaatioille pätee $\bar{\sigma} \circ \bar{\tau} \neq \bar{\tau} \circ \bar{\sigma}$ kuten tapauksessa $n = 3$. \square

Permutaatioilla operointia voi havainnollistaa monilla eri tavoilla. Proposition 10.1 todistuksessa käyttämämme tapa antaa permutaatio luettelemalla kaikkien alkioden kuvautuminen ei ole kovin kätevää. Seuraavat kaaviot havainnollistavat Proposition 10.1 todistuksessa esiintyvien permutaatioiden σ ja τ yhdistettyjä kuvauksia $\tau \circ \sigma$ ja $\sigma \circ \tau$:



Yksinkertaistamista varten otamme joillekin permutaatioille käyttöön tiiviimmän merkinnän:

Olkoon $\{a_1, a_2, \dots, a_m\} \subset \{1, 2, \dots, n\}$ m alkion osajoukko, $m \geq 2$.

Sykli $(a_1 a_2 \dots a_m)$ on permutaatio, joka kuvaa alkion a_i alkioiksi a_{i+1} kaikilla $i \in \{1, 2, \dots, m-1\}$, alkion a_m alkioiksi a_1 ja on identtinen kuvaus osajoukon $\{a_1, a_2, \dots, a_m\}$ komplementissa.

Syklin $(a_1 a_2 \dots a_m)$ **pituus** on m .

Jos syklin pituus on m , se on **m -sykli**.

Jos syklin pituus on 2, niin se on **vaihto** eli **transpositio** ja 2-sykli $(i \ i+1)$ on **alkeisvaihto** eli **alkeistranspositio**.

Sykliden $\sigma = (a_1 a_2 \dots a_m)$ ja $\tau = (b_1 b_2 \dots b_k)$, yhdistetty kuvaus on niiden **tulo**. Sykliden yhdistettyä kuvausta merkitään

$$\sigma \circ \tau = (a_1 a_2 \dots a_m)(b_1 b_2 \dots b_k).$$

Syklit $(a_1 a_2 \dots a_m)$ ja $(b_1 b_2 \dots b_k)$ ovat **erilliset**, jos

$$\{a_1, a_2, \dots, a_m\} \cap \{b_1, b_2, \dots, b_k\} = \emptyset.$$

Esimerkki 10.2. (1) Kaikki Proposition 10.1 todistuksessa esiintyvät kuvaukset ovat syklejä: $\sigma = (12)$, $\tau = (23)$, $\tau \circ \sigma = (23)(12) = (132)$ ja $\sigma \circ \tau = (12)(23) = (123)$. Loput permutaatioryhmän S_3 alkiot ovat vaihto (13) ja identtinen kuvaus.

(2) Kaikki syklin identtisestä kuvauksesta poikkeavat potenssit eivät välttämättä ole syklejä. Esimerkiksi $(1234)^2 = (1234)(1234) = (13)(24)$.

(3) $(a_k a_{k-1} \dots a_1)(a_1 a_2 \dots a_k) = \text{id}$ kaikille $a_1, \dots, a_k \in \{1, 2, \dots, n\}$, joten

$$(a_1 a_2 \dots a_k)^{-1} = (a_k a_{k-1} \dots a_1).$$

Lemma 10.3. *Erilliset syklit kommutoivat.*

Todistus. Jos σ ja σ' ovat erillisiä, ne ovat kahden toisiaan leikkaamattoman osajoukon permutaatioita, joten väite pätee selvästi. \square

Jos $f: X \rightarrow X$ on kuvaus ja $x \in X$, niin pisteen x **rata** (kuvauksella f) on

$$\mathcal{O}(x) = \mathcal{O}_f(x) = \bigcup_{n \in \mathbb{N}} \{f^n(x)\}.$$

Lemma 10.4. *Jokaisen m -syklin kertaluku on m .*

Todistus. Olkoon $\sigma = (a_1 a_2 \cdots a_m)$. Pisteen a_1 rata

$$\begin{aligned} \mathcal{O}(a_1) &= \{a_1, \sigma(a_1) = a_2, \sigma^2(a_1) = a_3, \dots, \sigma^{m-1}(a_1) = a_m, \sigma(a_m) = a_1, \dots\} \\ &= \{a_1, \sigma(a_1) = a_2, \sigma^2(a_1) = a_3, \dots, \sigma^{m-1}(a_1) = a_m\} \end{aligned}$$

koostuu m pisteestä ja sama pätee kaikille muillekin pisteille a_2, \dots, a_m . Siis kuvaukset σ^k , $k \in \{2, 3, \dots, m-1\}$, eivät ole identtisiä kuvauksia ja $\sigma^m = \text{id}$. Väite seuraa tästä. \square

10.2 Symmetrisen ryhmän rakenteesta

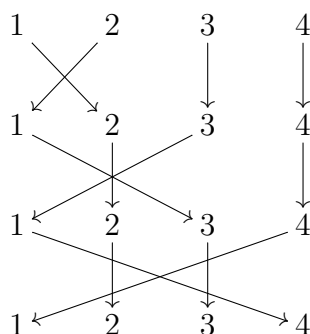
Tarkastelemme seuraavaksi symmetrisen ryhmän S_n rakennetta.

Propositio 10.5. *Jokainen sykli on vaihtojen tulo.*

Todistus. Induktiolla on helppo osoittaa, että

$$(a_1 a_2 \cdots a_m) = (a_1 a_m)(a_1 a_{m-1}) \cdots (a_1 a_2).$$

Todistuksen idea sisältyy seuraavaan kaavioon:



Yksityiskohdat harjoitustehtävässä 10.5. \square

Propositio 10.6. *Jokainen vaihto on alkeisvaihtojen pariton tulo.*

Todistus. Koska

$$(km) = (1k)(1m)(1k)$$

kaikilla $k, m \in \{2, 3, \dots, n\}$, $k \neq m$, riittää osoittaa, että $(1k)$ on alkeisvaihtojen pariton tulo kaikilla $k \in \{2, 3, \dots, n\}$. Vaihto (12) on alkeellinen. Oletetaan, että $(1 k - 1)$ on alkeisvaihtojen pariton tulo. Väite seuraa, koska

$$(1k) = (1 k - 1)(k - 1 k)(1 k - 1). \quad \square$$

Propositio 10.7. *Jokainen identtisestä kuvauksesta poikkeava permutaatio voidaan esittää erillisten syklien tulona.*

Todistus. Jos permutaatio τ kiinnittää pisteet $a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\}$, riittää todistaa väite permutaation τ rajoittumalle joukkoon $\{1, 2, \dots, n\} - \{a_1, a_2, \dots, a_k\}$. Riittää siis tarkastella permutaatioita, jotka eivät kiinnitä yhtään pistettä.

Selvästi väite pätee, kun $n = 2$. Oletetaan, että se pätee kaikilla S_k , kun $k \leq n - 1$. Olkoon $\tau \in S_n$. Jos τ on sykli ei ole mitään todistettavaa, joten voimme olettaa, että τ ei ole sykli. Piste 1 rata on

$$\mathcal{O}(1) = \{1, \tau(1), \tau^2(1), \dots, \tau^k(1), \dots\}.$$

Koska $\{1, \dots, n\}$ on äärellinen joukko, niin täytyy olla $\tau^q(1) = \tau^r(1)$ joillain luonnollisilla luvuilla $q < r$. Valitaan luvut q ja r niin, että ne ovat pienimmät mahdolliset. Koska τ on bijektio, täytyy olla $q = 0$, $\tau^r(1) = 1$: Jos nimittäin $q > 1$, niin

$$\tau(\tau^{r-1}(1)) = \tau^q(1) = \tau(\tau^{q-1}(1)),$$

joten bijektiivisyyden nojalla $\tau^{r-1}(1) = \tau^{q-1}(1)$, mikä on ristiriidassa lukujen q ja r minimalisuuden kanssa. Tästä nähdään, että

$$\tau|_{\mathcal{O}(1)} = (1 \ \tau(1) \ \tau^2(1) \ \dots \ \tau^{r-1}(1)).$$

Induktio-oletuksen nojalla permutaation τ rajoittuma osajoukkoon $\{1, 2, \dots, n\} - \mathcal{O}(1)$ on syklien tulo, joten väite on todistettu. \square

Lause 10.8. *(Alkeis)vaihdot virittävät symmetrisen ryhmän S_n .*

Todistus. Seuraa Propositioista 10.5, 10.6 ja 10.7. \square

10.3 Cayleyn lause

Osoitamme seuraavaksi, että kaikki ryhmät voi halutessa ajatella permutaatioryhmien aliryhminä, äärettömät ryhmät tietenkin äärettömien joukkojen permutaatioryhmien.

Olkoon G ryhmä ja olkoon $g \in G$. Kuvaus $\ell_g: G \rightarrow G$, $\ell_g(x) = gx$ kaikilla $x \in G$, on **vasen siirto** alkiolla $g \in G$.

Lemma 10.9. *Vasen siirto on bijektio.*

Todistus. Olkoon $g \in G$. Kuvaus $\ell_g: G \rightarrow G$ on surjektio, koska $\ell_g(g^{-1}z) = z$ kaikilla $z \in G$ ja supistussäännön nojalla se on injektio: Jos $\ell_g(x) = \ell_g(y)$, niin $gx = gy$, joten supistussäännön nojalla $x = y$. \square

Propositio 10.10. *Ryhmä G on isomorfinen ryhmän $\text{Perm}(G)$ jonkin aliryhmän kanssa.*

Todistus. Lemman 10.9 nojalla voidaan määritellä kuvaus $\rho: G \rightarrow \text{Perm}(G)$, $\rho(g) = \ell_g$. Kaikille $x \in G$ pätee

$$\rho(gh)(x) = \ell_{gh}(x) = (gh)x = g(hx) = \ell_g \circ \ell_h(x) = \rho(g) \circ \rho(h)(x).$$

Siis $\rho(gh) = \rho(g) \circ \rho(h)$, joten kuvaus ρ on homomorfismi.

Olkoot sitten $g, h \in G$ siten, että $\rho(g) = \rho(h)$. Tällöin

$$g = \ell_g(e) = \ell_h(e) = h,$$

joten ρ on injektio ja täten $\rho: G \rightarrow \rho(G) < \text{Perm}(G)$ on isomorfismi. \square

Lause 10.11 (Cayleyn lause). *Olkoon G äärellinen ryhmä, jonka kertaluku on n . Symmetrisellä ryhmällä S_n on aliryhmä, joka on isomorfinen ryhmän G kanssa.*

Todistus. Ryhmät S_n ja $\text{Perm}(G)$ ovat isomorfisia, joten voimme käsitellä ryhmää $\text{Perm}(G)$ ja väite seuraa Propositioista 10.10 \square

Esimerkki 10.12. Olkoon G ryhmä. Propositiossa 10.9 määrittelimme ryhmän G uskollisen toiminnan joukolla G asettamalla $\rho(g) = \ell_g$.

10.4 Permutaation merkki

Jokaiseen permutaatioon liittyvä tärkeä invariantti on permutaation merkki:

Permutaatio $\sigma \in S_n$ on **parillinen**, jos se on tulo parillisesta määrästä vaihtoja ja **pariton**, jos se on tulo parittomasta määrästä vaihtoja. Permutaation σ **merkki** on

$$\varepsilon(\sigma) = \begin{cases} -1, & \text{jos } \sigma \text{ on pariton} \\ 1, & \text{jos } \sigma \text{ on parillinen.} \end{cases}$$

Proposition 10.6 nojalla permutaatio on tulo parillisesta määrästä vaihtoja, jos ja vain jos se on tulo parillisesta määrästä alkeisvaihtoja.

Esimerkki 10.13. Permutaatiot ja niiden merkit esiintyvät lineaarialgebrassa determinanttien yhteydessä: Neliömatriisin $A = (a_{ij})_{i=1}^n$ determinantti on

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}.$$

Jos neliömatriisien vektoriavaruus $M_n(\mathbb{R})$ samastetaan avaruudeksi $(\mathbb{R}^n)^n$ esittämällä matriisi $A \in M_n(\mathbb{R})$ sarakkeidensa tai riviensä avulla muodossa

$$A = (v_1 \cdots v_n) = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix},$$

niin determinantti on antisymmetrinen kuvaus $\det: (\mathbb{R}^n)^n \rightarrow \mathbb{R}$:

$$\det(v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}) = \det \begin{pmatrix} w_{\sigma(1)} \\ w_{\sigma(2)} \\ \vdots \\ w_{\sigma(n)} \end{pmatrix} = \varepsilon(\sigma) \det A.$$

Osoitetaan, että permutaation merkki on hyvin määritelty kuvaus. Apuna käytetään antisymmetrisiä kuvauksia:

Olkoon X epätyhjä joukko ja olkoon $(V, +)$ additiivinen ryhmä. Kuvaus $f: X^n \rightarrow V$ on **antisymmetrinen**, jos kaikille alkeisvaihdolle $\tau \in S_n$ pätee

$$f(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) = -f(x).$$

On hyvä tuntea ainakin yksi esimerkki antisymmetrisestä funktiosta, joka ei ole nol-lafunktio. Seuraava tulos antaa tällaisen.

Lemma 10.14. *Kuvaus $f: \mathbb{Z}^n \rightarrow \mathbb{Z}$,*

$$f(x) = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

on antisymmetrinen. Lisäksi f ei ole nollakuvaus.

Todistus. Olkoon $1 \leq i_0 < n$ ja olkoon $\tau = (i_0 \ i_0 + 1)$. Tällöin

$$f(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) = (x_{i_0+1} - x_{i_0}) \prod_{\substack{1 \leq i < j \leq n \\ \{i,j\} \neq \{i_0, i_0+1\}}} (x_i - x_j) = -f(x),$$

sillä

- (1) jos $\{i, j\} \cap \{i_0, i_0 + 1\} = \emptyset$, niin permutaatio τ ei vaikuta termiin $x_i - x_j$,
- (2) jos $i < i_0$, niin molemmat termit $x_i - x_{i_0}$ ja $x_i - x_{i_0+1}$ esiintyvät tulossa ja permutaatio vaihtaa ne keskenään ja
- (3) jos $j > i_0 + 1$, niin molemmat termit $x_{i_0} - x_j$ ja $x_{i_0+1} - x_j$ esiintyvät tulossa ja permutaatio vaihtaa ne keskenään.

Lisäksi, kun muuttujan x komponentit ovat eri kokonaislukuja, $f(x) \neq 0$. □

Propositio 10.15. *Olkoon $f: X^n \rightarrow V$ antisymmetrinen kuvaus. Tällöin*

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = (-1)^r f(x),$$

jos σ on r alkeisvaihdon tulo.

Todistus. Väite pätee selvästi, kun $r = 1$. Oletetaan, että se pätee, kun σ on $r - 1$ alkeisvaihdon tulo. Olkoon $\sigma = \tau \circ \omega$ permutaatio, joka on r alkeisvaihdon tulo siten, että ω on $r - 1$ alkeisvaihdon tulo ja τ on alkeisvaihto. Nyt soveltamalla antisymmetrisyyden määritelmää alkeisvaihdolla τ ja pisteellä $(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$ saadaan

$$\begin{aligned} f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) &= f(x_{\tau(\omega(1))}, x_{\tau(\omega(2))}, \dots, x_{\tau(\omega(n))}) \\ &= -f(x_{\omega(1)}, x_{\omega(2)}, \dots, x_{\omega(n)}) = (-1)^r f(x). \end{aligned} \quad \square$$

Proposition 10.6 avulla saadaan välittömästi

Seuraus 10.16. Jos f on antisymmetrinen, niin kaikille vaihdoille $\tau \in S_n$ pätee

$$f(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) = -f(x). \quad \square$$

Propositio 10.17. Permutaation merkki on hyvin määritelty.

Todistus. Oletetaan, että permutaatio σ voidaan esittää r vaihdon tulona ja toisaalta s vaihdon tulona ja osoitetaan, että tällöin $r \equiv s \pmod{2}$. Olkoon $f: \mathbb{Z}^n \rightarrow \mathbb{Z}$,

$$f(x) = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

nollasta poikkeava antisymmetrinen funktio. Proposition 10.15 nojalla

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = (-1)^r f(x) = (-1)^s f(x),$$

kaikilla $x \in \mathbb{Z}^n$. Koska f ei ole nollafunktio, on $x \in \mathbb{Z}^n$, jolle $f(x) \neq 0$ ja saadaan $(-1)^r = (-1)^s$. Siis $r \equiv s \pmod{2}$. \square

Lause 10.18. Merkki $\varepsilon: S_n \rightarrow \{-1, 1\}$ on ainoa homomorfismi permutaatioryhmästä S_n multiplikatiiviseen ryhmään $\{-1, 1\}$, joka saa vaihdoilla arvon -1 .

Todistus. Olkoot $\sigma_1, \sigma_2 \in S_n$. Proposition 10.15 nojalla $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$, joten ε on homomorfismi.

Määritelmän mukaan $\varepsilon(\tau) = -1$ kaikille vaihdoille $\tau \in S_n$, joten merkki toteuttaa halutun ehdon. Toisaalta Lauseen 10.8 nojalla alkeisvaihdot virittävät ryhmän S_n , joten Proposition 9.15 nojalla homomorfismi $f: S_n \rightarrow \{-1, 1\}$ määräytyy, jos sen arvot tunnetaan tässä virittäjäjoukossa. Siis ε on ainoa homomorfismi, jolla on haluttu ominaisuus. \square

10.5 Alternoiva ryhmä A_n

Olkoon $n \geq 3$. Permutaatioiden merkkihomomorfismin $\varepsilon: S_n \rightarrow \{-1, 1\}$ ydin on **alternoiva ryhmä** A_n .

Alternoiva ryhmä koostuu parillisista permutaatioista. Se on symmetrisen ryhmän aito aliryhmä, koska $(12) \in S_n - A_n$ kaikille $n \geq 2$.

Propositio 10.19. Olkoon $n \geq 3$. Alternoivan ryhmän A_n kertaluku on $n!/2$.

Todistus. Olkoon $\tau \in S_n$ alkeisvaihto. Vasen siirto ℓ_τ on bijektio joukkojen A_n ja $S_n - A_n$ välillä. Siis $\#S_n = n! = 2 \#A_n$. \square

Esimerkki 10.20. (a) $(12 \cdots n) \in A_n$, jos ja vain jos n on pariton: $(123) = (13)(12)$, $(1234) = (14)(123)$ ja niin edelleen.

(b) $A_3 = \langle (123) \rangle < S_3$, $A_3 \cong C_3$.

(c) $A_4 = \langle (12)(34), (123) \rangle < S_4$. Permutaatiot $(12)(34)$ ja $(123) = (13)(12)$ ovat parillisia, joten $\langle (12)(34), (123) \rangle \leq A_4$. Yhtälön voi osoittaa laskemalla esimerkiksi, että

$$\begin{aligned} (12)(34)(123) &= (243), \\ (123)(12)(34) &= (134), \\ (12)(34)(123)(12)(34) &= (142) \end{aligned}$$

ja

$$(123)(241) = (13)(24),$$

$$(13)(24)(12)(34) = (14)(23).$$

Koska ryhmä $\langle (12)(34), (123) \rangle$ sisältää lisäksi identtisen kuvauksen ja edellä lueteltujen 3-sykliden neliöt, saadaan kaikki ryhmän A_4 12 alkioita.

Propositio 10.21. *Alternoiva ryhmä A_n on 3-sykliden virittämä.*

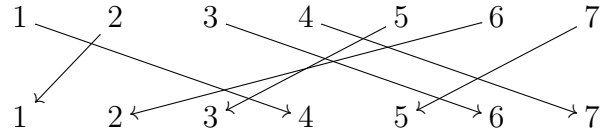
Todistus. Jokainen ryhmän A_n alkio on tulo parillisesta määrästä vaihtoja. Kahden vaihdon tuloille pätee $(xy)(xz) = (xzy)$ ja $(xy)(zt) = (xtz)(xyz)$, jos $x, y, z, t \in \{1, 2, \dots, n\}$ ja $\#\{x, y, z, t\} = 4$. Siis parillisen monen vaihdon tulo voidaan kirjoittaa 3-sykliden tulona. \square

Harjoitustehtäviä

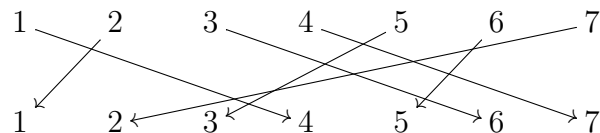
10.1. Olkoot X ja Y epätyhjiä joukkoja ja olkoon $f: X \rightarrow Y$ bijektio. Osoita, että permutaatioryhmät $\text{Perm}(X)$ ja $\text{Perm}(Y)$ ovat isomorfisia.

10.2. Osoita, että permutaatioryhmän S_n kertaluku on $n!$.

10.3. Kirjoita permutaatiot $(123)(24)$ ja $(1234)(235)$ ja kaavioita



ja



vastaavat permutaatiot erillisten syklien tuloina.

10.4. Olkoon $\sigma: \{1, 2, \dots, 7\} \rightarrow \{1, 2, \dots, 7\}$ permutaatio, jolle pätee

$$\sigma(1) = 3, \quad \sigma(2) = 5, \quad \sigma(3) = 7, \quad \sigma(4) = 1, \quad \sigma(5) = 6, \quad \sigma(6) = 2, \quad \sigma(7) = 4.$$

Kirjoita permutaatio σ erillisten syklien tulona.

10.5. Täydennä Proposition 10.5 todistus induktiotodistukseksi.

10.6. Osoita, että $S_3 = \langle (12), (23) \rangle$

10.7. Olkoon $n \geq 3$ ja olkoot $\alpha_n = (123 \cdots n)$ ja $\beta = (123)$. Määritä permutaatiot

$$\alpha_n(12x)\alpha_n^{-1} \quad \text{ja} \quad \beta^{-1}\alpha_n(12x)\alpha_n^{-1}\beta$$

jokaiselle $3 \leq x < n$.

10.8. Määritä permutaatiot

- $(1y2)(12x)(12y)$ kaikille $x, y \geq 3, x \neq y$ ja
- $(1xt)(1yz)(1tx)$ kaikille $x, y, t, z > 1$, kun $\#\{x, y, t, z\} = 4$.

10.9. Osoita, että jokaiselle parittomalle $n \geq 5$ pätee $A_n = \langle (123), (123 \dots n) \rangle$.²

10.10. Osoita, että $S_3 \cong \text{SL}_2(\mathbb{Z}/2\mathbb{Z})$.

10.11. Olkoon $n \geq 3$. Olkoot $a, b, c, d, e, f \in \{1, 2, \dots, n\}$ siten, että $a \neq b \neq c \neq a$ ja $d \neq e \neq f \neq d$. Osoita, että on $\sigma \in A_n$, jolle pätee $\{\sigma(a), \sigma(b), \sigma(c)\} = \{d, e, f\}$.³

²Käytä tehtävien 10.7 ja 10.8 tuloksia ja Propositiota 10.21.

³Tätä teknistä tulosta käytetään Harjoitustehtävässä 12.5.

Luku 11

Lagrangen lause

Tässä luvussa tarkastelemme ryhmän ja sen aliryhmien suhdetta. Otamme käyttöön luvussa 2.1 esitellyt osituksen ja ekvivalenssirelaation käsitteet. Aliryhmä $H < G$ määrää ryhmän G osituksen keskenään yhtä mahtavilla joukoilla. Tämä ositus antaa aliryhmän indeksin käsitteen, joka osoittautuu hyödylliseksi.

11.1 Sivuluokat

Olkoon G ryhmä ja olkoon $H \leq G$. Alkion $g \in G$ **vasen sivuluokka** (aliryhmän H suhteen) on

$$gH = \{gh : h \in H\}$$

ja sen **oikea sivuluokka** (aliryhmän H suhteen) on

$$Hg = \{hg : h \in H\}.$$

Aliryhmän H **vasempien sivuluokkien joukko** ryhmässä G on

$$G/H = \{gH : g \in G\}$$

ja **oikeiden sivuluokkien joukko** on^a

$$H \backslash G = \{Hg : g \in G\}.$$

^aMerkintää ei pidä sekoittaa joukkojen erotukseen.

Jos kommutatiivisen ryhmän G laskutoimitusta merkitään additiivisesti, niin aliryhmän $H \leq G$ sivuluokkia merkitään $x + H$ tai $H + x$.

Esimerkki 11.1. Aliryhmän $q\mathbb{Z} < \mathbb{Z}$ sivuluokkien joukko on kongruenssiluokkien joukko (modulo q). Tämä on selitys sille, miksi kongruenssiluokkien joukolle käytetään mer-

kintää $\mathbb{Z}/q\mathbb{Z}$. Aliryhmän $q\mathbb{Z} < \mathbb{Z}$ sivuluokille pätee

$$n + q\mathbb{Z} = \{n + kq : k \in \mathbb{Z}\} = \{kq + n : k \in \mathbb{Z}\} = q\mathbb{Z} + n.$$

Edellä tehty havainto vasemmista ja oikeista sivuluokista yleistyy kaikille kommutatiivisille ryhmille:

Lemma 11.2. *Olkoon G kommutatiivinen ryhmä. Tällöin jokaiselle $x \in G$ ja jokaiselle $H \leq G$ pätee $xH = Hx$.* \square

Esimerkki 11.3. Olkoon $H = \langle(12)\rangle < S_3$. Aliryhmän H vasemmat sivuluokat ovat

$$\begin{aligned} H &= (12)H = \{\text{id}, (12)\}, \\ (123)H &= (13)H = \{(123), (13)\} \quad \text{ja} \\ (132)H &= (23)H = \{(132), (23)\} \end{aligned}$$

Sen oikeat sivuluokat ovat

$$\begin{aligned} H &= H(12) = \{\text{id}, (12)\}, \\ H(123) &= H(23) = \{(123), (23)\} \quad \text{ja} \\ H(132) &= H(13) = \{(132), (13)\}. \end{aligned}$$

Harjoitustehtävissä 11.9 ja 11.10 tarkastellaan esimerkkiä ryhmästä, joka ei ole kommutatiivinen, vaikka sen kaikkien aliryhmien vasemmat ja oikeat sivuluokat ovat samoja joukkoja.

Propositio 11.4. *Olkoon G ryhmä ja olkoon $H \leq G$. Tällöin*

- (1) $xH = yH$, jos ja vain jos $y^{-1}x \in H$. Erityisesti $xH = H$, jos ja vain jos $x \in H$.
- (2) $Hx = Hy$, jos ja vain jos $xy^{-1} \in H$. Erityisesti $Hx = H$, jos ja vain jos $x \in H$.

Todistus. Harjoitustehtävä 11.2. \square

Kongruenssiluokat modulo q muodostavat kokonaislukujen ryhmän $(\mathbb{Z}, +)$ osituksen ja Esimerkissä 11.3 aliryhmän $H = \langle(12)\rangle$ vasemmat ja oikeat sivuluokat määräävät kaksi ryhmän $G = S_3$ ositusta. Seuraava tulos yleistää tämän havainnon.

Propositio 11.5. *Olkoon G ryhmä ja olkoon H sen aito aliryhmä. Tällöin*

- (1) Vasemmat sivuluokat muodostavat ryhmän G osituksen. Erityisesti, jos $x, y \in G$, niin $xH = yH$, jos ja vain jos $x \in yH$.
- (2) Oikeat sivuluokat muodostavat ryhmän G osituksen. Erityisesti, jos $x, y \in G$, niin $Hx = Hy$, jos ja vain jos $x \in Hy$.

Todistus. (1) Vasempien sivuluokkien yhdiste on koko G sillä $x \in xH$ kaikille $x \in G$. Jos $xH \cap yH \neq \emptyset$, niin on $h, h' \in H$, joille $xh = yh'$. Mutta tällöin, jos $g \in xH$, niin $g = xh''$ jollain $h'' \in H$, joten $g = xh'' = yh'h^{-1}h'' \in yH$. Vastaava päättely antaa inklusion toiseen suuntaan. Siis vasemmat sivuluokat muodostavat osituksen.

Väite (2) todistetaan samaan tapaan. \square

Olkoon $H \leq G$. Aliryhmän H määräämät relaatiot $\underset{\vee}{\sim}$ ja $\underset{\circ}{\sim}$ määritellään asettamalla

- $x \underset{\vee}{\sim} y$, jos ja vain jos $x^{-1}y \in H$ ja
- $x \underset{\circ}{\sim} y$, jos ja vain jos $yx^{-1} \in H$.

Propositio 11.6. *Olkoon $H \leq G$. Aliryhmän H määräämät relaatiot ovat ekvivalenssi-relaatioita joukossa G .*

Todistus. Proposition 11.4 nojalla relaatio $\underset{\vee}{\sim}$ on aliryhmän vasempien sivuluokkien määräämä relaatio, joka on Propositioiden 11.5 ja 2.3 nojalla ekvivalenssi-relaatio. Vastaavasti relaatio $\underset{\circ}{\sim}$ on oikeiden sivuluokkien määräämä ekvivalenssi-relaatio. \square

Propositio 11.7. *Olkoon G ryhmä ja olkoon $H \leq G$. Tällöin joukot H , gH ja Hg ovat yhtä mahtavia¹ kaikilla $g \in G$.*

Todistus. Lemman 10.9 nojalla vasen siirto $\ell_x: G \rightarrow G$ on bijektio. Vasemman sivuluokan määritelmän nojalla $\ell_x(H) = xH$. Vastaavasti oikea siirto $r_x: G \rightarrow G$, joka määritellään asettamalla $r_x(h) = hx$ kaikille $x \in G$, antaa bijektio joukkojen H ja Hx välille. \square

11.2 Aliryhmän indeksi ja Lagrangen lause

Propositio 11.8. *Olkoon G ryhmä ja olkoon $H \leq G$. Joukot G/H ja $H \setminus G$ ovat yhtä mahtavia.*

Todistus. Harjoitustehtävä 11.3 \square

Aliryhmän $H < G$ indeksi on^a

$$[G : H] = \#(G/H) = \#(H \setminus G).$$

^aPropositio 11.8 nojalla aliryhmän H indeksi voidaan määritellä kumman tahansa sivuluokkien joukon avulla.

Esimerkki 11.9. (a) $[\mathbb{Z} : q\mathbb{Z}] = q$.

(b) Aliryhmän $C_2 \times \{e\}$ indeksi ryhmässä $C_2 \times C_2$ on

$$[C_2 \times C_2 : C_2 \times \{e\}] = 2.$$

(c) $[\mathbb{R}^2 : \mathbb{R} \times \{0\}] = \infty$, sillä sivuluokat ovat $\mathbb{R} \times \{0\} + (0, a) = \mathbb{R} \times \{a\}$, $a \in \mathbb{R}$.

Lause 11.10 (Lagrangen lause). *Olkoon G äärellinen ryhmä ja olkoon $H < G$. Tällöin*

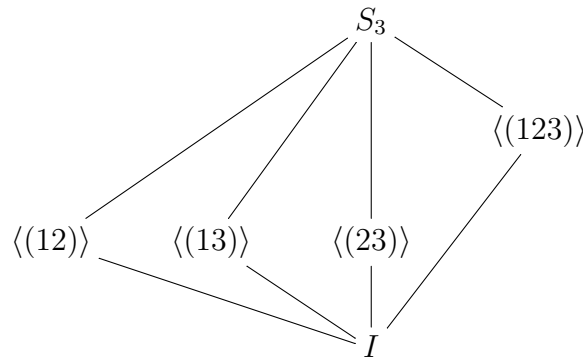
$$[G : H] = \frac{\#G}{\#H}.$$

Todistus. Proposition 11.5 nojalla kaikki sivuluokat ovat yhtä mahtavia ja sivuluokat osittavat ryhmän G . Siis $\#G = \#(G/H)\#H = \#(H \setminus G)\#H$, mistä väite seuraa. \square

¹Joukot A ja B ovat yhtä mahtavia, jos on bijektio $f: A \rightarrow B$.

Lagrange'n lauseen mukaan äärellisen ryhmän G aliryhmien indeksit ja kertaluvut ovat ryhmän kertaluvun tekijöitä. Esimerkissä 9.22 näimme, että ryhmällä $\mathbb{Z}/12\mathbb{Z}$ on kaikkien mahdollisten indeksien aliryhmät.

Esimerkki 11.11. Ryhmän S_3 kertaluku on 6, joten sen aliryhmien mahdolliset kertaluvut (ja indeksit) ovat 1, 2, 3 ja 6. Kolmen alkion permutaatioiden ryhmän aliryhmärakenne on yksinkertainen ja sitä voi havainnollistaa aliryhmäkaaviolla, jossa $I = \{\text{id}\}$.



Siis symmetrisellä ryhmällä S_3 on jokaista Lagrange'n lauseen sallimaa kokoa olevia aliryhmiä.

Esimerkki 11.12. Alternoivan ryhmän A_4 kertaluku on 12. Siis sen aidossa aliryhmässä voi Lagrange'n lauseen mukaan olla korkeintaan 6 alkioita. Esimerkin 10.20(c) päätelmä voidaan tehdä myös näin: Koska aliryhmä $\langle (12)(34), (123) \rangle$ sisältää 3-syklit (123) , (243) ja (134) ja niiden kaikki potenssit, niin siinä on ainakin 8 alkioita. Siis se on koko A_4 .

Esimerkissä 12.21 osoitetaan, että ryhmällä A_4 ei ole kuuden alkion aliryhmää vaikka Lagrange'n lauseen mukaan 6 on mahdollinen aliryhmän kertaluku.

Seuraus 11.13. Jos G on äärellinen ryhmä ja $g \in G$, niin $\text{ord } g$ on kertaluvun $\#G$ tekijä. \square

Seuraus 11.14. Jos ryhmän G kertaluku on alkuluku, niin G on syklinen.

Todistus. Olkoon $g \in G$ alkio, joka ei ole neutraalialkio. Tällöin $\text{ord } g > 1$ ja $\text{ord } g$ on kertaluvun $\#G$, joten $\text{ord } g = \#G$. Siis $\langle g \rangle = G$. \square

Propositio 11.15. Olkoon G äärellinen ryhmä. Tällöin $g^{\#G} = e$ jokaiselle $g \in G$.

Todistus. Seurauksen 11.13 mukaan $\#G = k \text{ ord } g$ jollain $k \in \mathbb{N}$, joten potenssisääntöjen ja Lemman 9.17 nojalla

$$g^{\#G} = g^{k \text{ ord } g} = (g^{\text{ord } g})^k = e^k = e. \quad \square$$

Seuraus 11.16. Olkoon G äärellinen ryhmä ja olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi. Tällöin

$$\#\phi(G) = [G : \ker \phi]$$

ja

$$\#G = \#\ker G \#\phi(G).$$

Todistus. Proposition 11.4 nojalla $x \ker \phi = y \ker \phi$, jos ja vain jos $y^{-1}x \in \ker \phi$. Tämä pätee, jos ja vain jos $\phi(x) = \phi(y)$. Siis kuvaus $x \ker \phi \mapsto \phi(x)$ on bijektio joukosta $G/\ker \phi$ joukkoon $\phi(G)$. Siis $\#\phi(G) = [G : \ker \phi]$ ja toinen väite seuraa Lagrange'n lauseesta. \square

Propositio 11.17. *Olkoon G ryhmä. Olkoot $K < H < G$ siten, että $[G : H] < \infty$ ja $[H : K] < \infty$. Tällöin*

$$[G : K] = [G : H][H : K].$$

11.3 Lagrangen lauseen sovelluksia lukuteoriaan

Tässä luvussa sovellamme Lagrangen lausetta lukuteoriaan.

Lause 11.18 (Fermat'n pieni lause). *Olkoon p alkuluku. Kaikille $a \in \mathbb{Z}$ pätee $a^p \equiv a \pmod{p}$.*

Todistus. Proposition 8.22 nojalla ryhmässä $(\mathbb{Z}/p\mathbb{Z})^\times$ on $p - 1$ alkioita. Proposition 11.15 nojalla $(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$, joten

$$a^p + p\mathbb{Z} = (a + p\mathbb{Z})^p = a + p\mathbb{Z}.$$

Siis $a^p - a \in p\mathbb{Z}$, mikä on yhtäpitävää väitteen kanssa. □

Lemma 11.19. *Jos p on alkuluku, $p \equiv 3 \pmod{4}$, niin $-1 + p\mathbb{Z}$ ei ole minkään alkion neliö ryhmässä $(\mathbb{Z}/p\mathbb{Z})^\times$.*

Todistus. Jos $-1 + p\mathbb{Z} = (a + p\mathbb{Z})^2$, niin $(a + p\mathbb{Z})^4 = 1$, joten Seurauksen 11.13 nojalla $\#(\mathbb{Z}/p\mathbb{Z})^\times \equiv 0 \pmod{4}$ mutta oletuksen nojalla $\#(\mathbb{Z}/p\mathbb{Z})^\times \equiv 2 \pmod{4}$. □

Propositio 11.20. *Olkoon p alkuluku, $p \equiv 3 \pmod{4}$. Osoita, että $X^2 + 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ on jaoton polynomi.*

Todistus. Proposition 6.16 nojalla $X^2 + 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ on jaoton, jos ja vain jos sillä ei ole juurta. Lemman 11.19 sillä ei ole juurta. □

Harjoitustehtäviä

11.1. Osoita, että $\mathbb{R}_+ < \mathbb{C}^\times$ ja määritä aliryhmän \mathbb{R}_+ sivuluokat ryhmässä \mathbb{C}^\times . Piirrä kuva, joka havainnollistaa sivuluokkien määräämää ositusta.

11.2. Todista Propositio 11.4.

11.3. Olkoon G ryhmä ja olkoon $H < G$. Osoita, että tekijäjoukkojen välinen kuvaus $b : G/H \rightarrow H \backslash G$, $b(aH) = Ha^{-1}$ on bijektio.

11.4. Olkoot $c, d \in \mathbb{Z}$ siten, että c jakaa luvun d . Laske indeksi $[c\mathbb{Z} : d\mathbb{Z}]$.

11.5. Määritä kaikki ryhmien $(\mathbb{Z}/6\mathbb{Z}, +)$ ja $(\mathbb{Z}/7\mathbb{Z}, +)$ aliryhmät.

11.6. Piirrä ryhmän $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ aliryhmäkaavio.

11.7. Olkoon G äärellinen ryhmä. Olkoot $K < H < G$. Osoita Lagrangen lauseen avulla, että indekseille pätee:

$$[G : K] = [G : H][H : K].$$

11.8. Todista Propositio 11.17.²

²Tässä ei oleteta, että G on äärellinen, joten Lagrangen lausetta ei voi käyttää.

Ryhmä

$$Q_8 = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\} \leq \mathbb{H}^\times$$

on kvaternioryhmä Q_8 .^a

^aRyhmä \mathbb{H}^\times on Hamiltonin kvaternioiden multiplikatiivinen ryhmä, katso luku 4.3.

11.9. Osoita, että $Q_8 \leq \mathbb{H}^\times$.

11.10. Piirrä ryhmän Q_8 aliryhmäkaavio.

11.11. Olkoon G ryhmä, jossa on korkeintaan 5 alkioita. Osoita, että G on kommutatiivinen.³

11.12. Määritä aliryhmä $\langle (123), (124) \rangle \leq A_4$.

11.13. Osoita, että $S_4 = \langle (12), (1234) \rangle$.⁴

11.14. Olkoon p alkuluku. Osoita, että kunta $\mathbb{Z}/p\mathbb{Z}$ ei ole algebrallisesti suljettu⁵

11.15. Olkoon $p > 3$ alkuluku. Osoita, että $1 + p\mathbb{Z}$ ja $-1 + p\mathbb{Z}$ ovat ainoat kunnan $\mathbb{Z}/p\mathbb{Z}$ alkioita, jotka ovat omat käänteisalkionsa kertolaskun suhteen.⁶ Osoita, että

$$(2 + p\mathbb{Z})(3 + p\mathbb{Z}) \cdots (p - 2 + p\mathbb{Z}) = 1 + p\mathbb{Z}.$$

11.16. Osoita, että

$$(p - 1)! \equiv -1 \pmod{p},$$

jos p on alkuluku.

11.17. Osoita, että

$$(q - 1)! \equiv 0 \pmod{q}$$

jos $q \geq 6$ ei ole alkuluku.

11.18. Olkoon p pariton alkuluku ja olkoon $k = \frac{p-1}{2}$. Osoita, että

$$(p - 1)! = (-1)^k (k!)^2 \pmod{p}.$$

Osoita, että polynomi $X^2 + 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ ei ole jaoton, jos $p \equiv 1 \pmod{4}$.

11.19. Olkoon $n \in \mathbb{N} - \{0\}$ ja olkoon \mathcal{R}_n niiden laskutoimitusten $*$ joukko, joille laskutoimituksella varustettu joukko $(\{1, 2, \dots, n\}, *)$ on ryhmä. Määritellään joukossa \mathcal{R}_n relaatio \sim asettamalla $* \sim \circ$, jos ja vain jos ryhmät $(\{1, 2, \dots, n\}, *)$ ja $(\{1, 2, \dots, n\}, \circ)$ ovat isomorfisia. Osoita, että relaatio \sim on ekvivalenssirelaatio.⁷

³Kertaluku 4 teettää eniten työtä.

⁴Käytä Lagrange'n lausetta.

⁵Katso luku 6.7. Montako juurta polynomilla $X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ on?

⁶Lause 6.20.

⁷Palauta mieleen ryhmien isomorfismin määritelmä luvusta 8.3.

Luku 12

Normaalit aliryhmät ja tekijäryhmät

Tässä luvussa tarkastelemme aliryhmiä, joiden suhteen muodostettujen sivuluokkien joukossa on luonnollinen tekijäryhmän rakenne.

12.1 Normaalit aliryhmät

Ryhmän G aliryhmä H on **normaali**, jos $gH = Hg$ kaikille $g \in G$. Jos H on ryhmän G normaali aliryhmä, merkitään $H \trianglelefteq G$, aitoa normaalia aliryhmää merkitään $H \triangleleft G$.

Lemma 12.1. *Olkoon $K \trianglelefteq G$ ja $K < H < G$. Tällöin $K \trianglelefteq H$.* □

Esimerkki 12.2. (a) Ryhmä itse ja neutraalialkion muodostama aliryhmä ovat normaaleja aliryhmiä.

(b) Jos g on kommutatiivinen ryhmä, niin Lemman 11.2 mukaan sen kaikki aliryhmät ovat normaaleja. Erityisesti $q\mathbb{Z} \triangleleft (\mathbb{Z}, +)$ ja $\mathbb{R} \times \{0\} \triangleleft (\mathbb{R}^2, +)$.

(c) Esimerkissä 11.3 osoitettiin, että aliryhmä $\langle(12)\rangle < S_3$ ei ole normaali.

Joissain tilanteissa normaalius on helppo tarkastaa:

Propositio 12.3. *Jos $[G : H] = 2$, niin $H \triangleleft G$.*

Todistus. Vasemmat sivuluokat ovat H ja $G - H$, samoin oikeat sivuluokat. □

Esimerkki 12.4. Olkoon $n \geq 3$. Lagrangen lauseen nojalla $[S_n : A_n] = 2$, joten Proposition 12.3 nojalla $A_n \triangleleft S_n$ kaikilla $n \geq 3$. Erityisesti $C_3 \cong \langle(123)\rangle = A_3 \triangleleft S_3$.

Usein on kätevä käyttää seuraavaa normaalin aliryhmän karakterisointia:

Propositio 12.5. *Ryhmän G aliryhmä H on normaali, jos ja vain jos $ghg^{-1} \in H$ kaikilla $h \in H$ ja kaikilla $g \in G$*

Todistus. Jos H on normaali, niin $gH = Hg$ kaikille $g \in G$. Siis jokaiselle $g \in G$ ja $h \in H$ pätee $gh = h'g$ jollain $h' \in H$, joten $ghg^{-1} = h' \in H$.

Jos taas kaikille $g \in G$ ja $h \in H$ pätee $ghg^{-1} \in H$, niin jokaiselle $g \in G$ ja $h \in H$ on $h' \in H$, jolle $ghg^{-1} = h'$. Siis $gh = h'g \in Hg$, joten $gH \subset Hg$ kaikille $g \in G$. Samoin saadaan $hg^{-1} \in g^{-1}H$, joten $Hg^{-1} \subset g^{-1}H$ kaikille $g \in G$. Koska jokainen ryhmän G alkio on jonkin alkion käänteisalkio, väite on todistettu. \square

Esimerkki 12.6. Jos $\alpha \in A_n < S_n$ on parillinen permutaatio ja $\beta \in S_n$ on permutaatio, niin $\beta\alpha\beta^{-1}$ on parillinen permutaatio. Siis Propositio 12.5 antaa toisen todistuksen sille, että $A_n \triangleleft S_n$.

Sovellamme Propositiota 12.5, kun osoitamme, että normaalit aliryhmät sopivat hyvin yhteen homomorfismien kanssa.

Propositio 12.7. *Olkoon $\phi: G \rightarrow G'$ ryhmähomomorfismi.*

(1) *Olkoon $H \trianglelefteq G$. Tällöin $\phi(H) \trianglelefteq \phi(G) = \text{Im } \phi$.*

(2) *Olkoon $H' \trianglelefteq G'$. Tällöin $\phi^{-1}(H') \trianglelefteq G$.*

Todistus. (1) Proposition 9.7 nojalla $\phi(H) \leq \phi(G)$. Olkoot $a' \in \phi(H)$ ja $g' \in \phi(G)$. Tällöin on $a \in H$ ja $g \in G$, joille $a' = \phi(a)$ ja $g' = \phi(g)$. Nyt

$$g'a'(g')^{-1} = \phi(g)\phi(a)\phi(g)^{-1} = \phi(gag^{-1}) \in \phi(H),$$

koska $gag^{-1} \in H$. Väite seuraa Proposition 12.5 nojalla.

(2) Harjoitustehtävä 12.1. \square

Propositioista 12.7 saadaan tärkeänä erikoistapauksena

Seuraus 12.8. *Ryhmähomomorfismin ydin on normaali aliryhmä.* \square

Esimerkki 12.9. (a) $A_n = \ker \varepsilon \triangleleft S_n$.

(b) $\text{SL}_n(\mathbb{R}) = \ker \det \triangleleft \text{GL}_n(\mathbb{R})$.

(c) $\text{SO}(n) = \ker \det|_{\text{O}(n)} \triangleleft \text{O}(n)$

Propositio 12.7 kohdassa (1) on syytä pitää mielessä, että $\phi(H)$ ei välttämättä ole ryhmän G' normaali aliryhmä: Jos $H < G$ on aliryhmä, joka ei ole normaali ja jos $\phi: H \rightarrow G$ on inklusiokuvaus, ei tietenkään $\phi(H) = H$ ole ryhmän G normaali aliryhmä.

12.2 Tekijäryhmät

Propositioiden 11.5 ja 2.3 mukaan ryhmän G normaalin aliryhmän H vasemmat sivuluokat määräävät ekvivalenssirelaation, jonka ekvivalenssiluokat ovat vasemmat sivuluokat ja vastaavasti oikeat sivuluokat määräävät ekvivalenssirelaation, jonka ekvivalenssiluokat ovat oikeat sivuluokat. Koska normaalin aliryhmän H vasemmat ja oikeat sivuluokat määräävät saman osituksen ryhmälle G , ne määräävät saman ekvivalenssirelaation $\sim_v = \sim_o = \sim$.

Seuraava tulos on jatkon kannalta oleellinen:

Lause 12.10. *Olkoon G ryhmä ja olkoon $H \trianglelefteq G$. Tällöin sivuluokkien määräämä ekvivalenssirelaatio on yhteensopiva ryhmän G laskutoimituksen kanssa.*

Todistus. Olkoot $x, x', y, y' \in G$ siten, että $x \sim x'$ ja $y \sim y'$. Tällöin siis $x' \in xH$ ja $y' \in yH$, joten on $h_1, h_2 \in H$, joille $x' = xh_1$, $y' = yh_2$. Koska H on normaali, on $h_3 \in H$, jolle $h_1y = yh_3$. Siis

$$x'y' = xh_1yh_2 = xyh_3h_2 \in xyH,$$

joten $xy \sim x'y'$ ja laskutoimitus on yhteensopiva sivuluokkien määräämän ekvivalenssirelaation kanssa. \square

Jos G on multiplikaatiivinen ryhmä ja $N \trianglelefteq G$, niin tekijälaskutoimitus on

$$(aH)(bH) = abH$$

kaikille $a, b \in G$. Additiivisen ryhmän $(A, +)$ alkion x sivuluokalle käytetään merkintää $x + H$ ja tekijälaskutoimitus on siis tällä merkintätavalla

$$(x + H) + (y + H) = (x + y) + H$$

kaikille $x, y \in A$.

Seuraus 12.11. Jos $H \trianglelefteq G$, niin tekijäjoukko G/H varustettuna tekijälaskutoimituksella on ryhmä. Tekijäryhmän G/H neutraalialkio on H .

Todistus. Tekijälaskutoimituksen assosiativisuus osoitettiin Propositionissa 2.7. Koska luonnollinen homomorfismi on surjektiivinen, niin Proposition 2.7 nojalla se kuvaa ryhmän G neutraalialkion tekijälaskutoimituksen neutraalialkioksi, joka siis on $H \in G/H$. Tekijälaskutoimituksen määritelmän mukaan kaikille $gH \in G/H$ pätee $(gH)(g^{-1}H) = H$, joten laskutoimituksella varustetun joukon G/H jokaisella alkiolla on käänteisalkio. \square

Ryhmä G/H on normaalin aliryhmän H määräämä ryhmän G tekijäryhmä.

Esimerkki 12.12. Ryhmä $\mathbb{Z}/q\mathbb{Z}$ on kongruenssia mod q vastaava kokonaislukujen ryhmän tekijäryhmä.

Propositio 12.13. Olkoon G ryhmä ja olkoon $H \leq G$. Jos ryhmän G laskutoimitus on yhteensopiva ekvivalenssirelaation $\underset{v}{\sim}$ tai $\underset{o}{\sim}$ kanssa, niin H on normaali.

Todistus. Oletetaan, että laskutoimitus on yhteensopiva ekvivalenssirelaation $\underset{v}{\sim}$ kanssa. Kuten Seurauksen 12.11 todistuksessa, G/H varustettuna tekijälaskutoimituksella on ryhmä, jonka neutraalialkio on H . Luonnollinen homomorfismi $\pi: G \rightarrow G/H$ on ryhmähomomorfismi ja sen ydin on $H \leq G$. Proposition 12.7 nojalla H on normaali.

Toinen tapaus todistetaan samaan tapaan. \square

Sykliset ryhmät käyttäytyvät hyvin tekijäryhmienkin suhteen

Propositio 12.14. Jokainen syklisen ryhmän tekijäryhmä on syklinen.

Todistus. Olkoon $G = \langle v \rangle$ ja olkoon $H \trianglelefteq G$. Tällöin

$$G/H = \{gH : g \in G\} = \{v^k H : k \in \mathbb{Z}\} = \{(vH)^k : k \in \mathbb{Z}\} = \langle vH \rangle. \quad \square$$

Esimerkki 12.15. Harjoitustehtävässä 12.3 osoitetaan, että $Z(G)$ on ryhmän G normaali aliryhmä. Jos G on kommutatiivinen, niin $Z(G) = G$, joten tekijäryhmä $G/Z(G)$ kuvaa ryhmän G epäkommutatiivisuutta.

Propositio 12.16. *Olkoon G ryhmä. Aliryhmä $H \leq G$ on normaali aliryhmä, jos ja vain jos se on jonkin ryhmässä G määritellyn ryhmähomomorfismin ydin.*

Todistus. Harjoitustehtävä 12.7. □

12.3 Ryhmien ensimmäinen isomorfismilause

Todistamme seuraavaksi tärkeimmän tekijäryhmiä koskevan tuloksen. Todistus on Lauseen 9.20(1) todistuksen yleistys ja itse asiassa sama kuin renkaiden isomorfismilauseen¹ todistus.

Lause 12.17 (Ryhmien (ensimmäinen) isomorfismilause). *Jos $\phi: G \rightarrow G'$ on ryhmähomomorfismi, niin $\text{Im } \phi \cong G/\ker \phi$.*

$$\begin{array}{ccc} G & & \\ \downarrow \pi & \searrow \phi & \\ G/\ker \phi & \xrightarrow[\cong]{\psi} & G' \end{array}$$

Todistus. Jos $x \ker \phi = y \ker \phi$, niin Proposition 11.5 nojalla jollain $h \in \ker \phi$ pätee $y = xh$. Siis

$$\phi(y) = \phi(xh) = \phi(x)\phi(h) = \phi(x)e' = \phi(x).$$

Tähän havaintoon perustuen määritellään kuvaus $\psi: G/\ker \phi \rightarrow \text{Im } \phi$,

$$\psi(x \ker \phi) = \phi(x),$$

joka on homomorfismi: Olkoot $x, y \in G$. Tällöin

$$\psi(x \ker \phi)\psi(y \ker \phi) = \phi(x)\phi(y) = \phi(xy) = \psi(xy \ker \phi) = \psi(x \ker \phi y \ker \phi).$$

Kuvaus ψ on selvästi surjektio. Osoitetaan se vielä injektiksi. Olkoot $x, y \in G$ siten, että

$$\phi(x) = \psi(x \ker \phi) = \psi(y \ker \phi) = \phi(y).$$

Tällöin $x^{-1}y \in \ker \phi$, joten Proposition 11.4 nojalla $x \ker \phi = y \ker \phi$. □

Seuraus 12.18. *Olkoon $\phi: G \rightarrow G'$ surjektiivinen ryhmähomomorfismi. Tällöin $G' \cong G/\ker \phi$.* □

Lause 12.19. *Olkoon $\phi: G \rightarrow G'$ surjektiivinen ryhmähomomorfismi ja olkoon $H' \trianglelefteq G'$. Tällöin $G/\phi^{-1}(H') \cong G'/H'$.*

Todistus. Proposition 12.7(2) mukaan $H = \phi^{-1}(H') \trianglelefteq G$. Olkoon $\pi: G \rightarrow G'/H'$ luonnollinen homomorfismi. Tällöin $\tilde{\psi} = \pi \circ \phi: G \rightarrow G'/H'$ on surjektiivinen homomorfismi, jonka ydin on H . Lauseen 12.17 mukaan $G/H \cong G'/H'$. □

¹Lause 7.19

Esimerkki 12.20. (a) Homomorfismi $\phi: \mathbb{Z}^2 \rightarrow (\mathbb{Z}/2\mathbb{Z})^2$,

$$\phi(k_1, k_2) = (k_1 + 2\mathbb{Z}, k_2 + 2\mathbb{Z}),$$

on surjektio, jonka ydin on $(2\mathbb{Z})^2 \triangleleft \mathbb{Z}^2$. Isomorfismilauseen nojalla $\mathbb{Z}^2/(2\mathbb{Z})^2$ on isomorfinen ryhmän $K_4 = (\mathbb{Z}/2\mathbb{Z})^2$ kanssa. Siis

$$[\mathbb{Z}^2 : (2\mathbb{Z})^2] = \#((\mathbb{Z}/2\mathbb{Z})^2) = \#K_4 = 4.$$

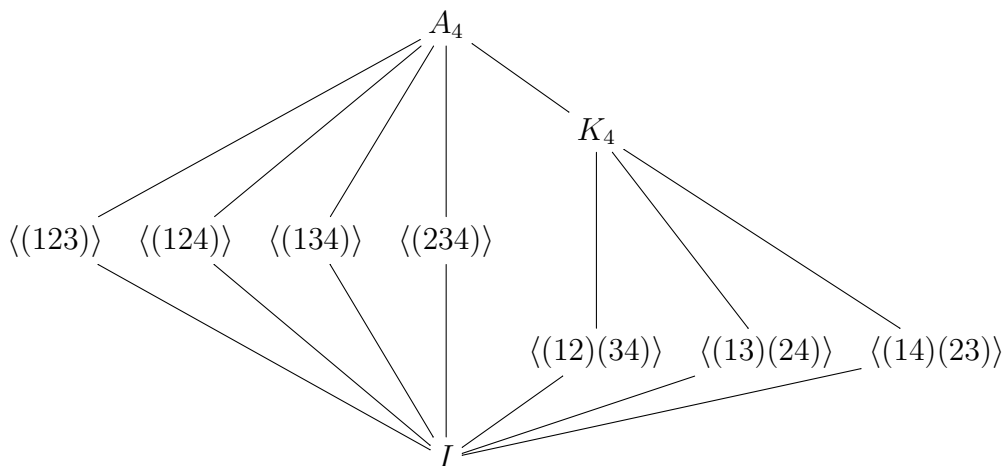
(b) Kuvaus $\phi: \mathbb{R} \rightarrow \mathbb{S}^1 < \mathbb{C}^\times$, $\phi(t) = \cos(2\pi t) + i \sin(2\pi t)$, on surjektiivinen homomorfismi, jonka ydin on selvästi \mathbb{Z} . Siis $\mathbb{S}^1 \cong \mathbb{R}/\mathbb{Z}$.

(c) Olkoon $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Tällöin $\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \cong \mathbb{K}^\times$, koska $\det \mathrm{GL}_n(\mathbb{K}) \rightarrow \mathbb{K}^\times$ on surjektiivinen homomorfismi, jonka ydin on $\mathrm{SL}_n(\mathbb{K})$.

Esimerkki 12.21. Esimerkissä 11.12 osoitimme, Osoitamme nyt, että alternoivalla ryhmällä A_4 ei ole kuuden alkion aliryhmää. Jos $H < A_4$ on aliryhmä, jonka kertaluku on 6, niin Lagrangen lauseen mukaan $[A_4 : H] = 2$. Proposition 12.3 nojalla $H \triangleleft A_4$. Tekijäryhmässä A_4/H on kaksi alkioita, joten $A_4/H \cong \mathbb{Z}/2\mathbb{Z}$. Siis kaikille $g \in G$ pätee $g^2H = gHgH = H$, joten Proposition 11.4 nojalla $g^2 \in H$ kaikille $g \in G$.

Kaikki 3-syklit kuuluvat ryhmään A_4 Esimerkin 10.20 nojalla. Jos $g \in A_4$ on 3-sykli, niin $g = g^4 = (g^2)^2 \in H$. Kaikki 3-syklit siis sisältyvät aliryhmään H . Proposition 10.21 nojalla $H = A_4$. Päätelmän voi tehdä myös ilman Propositiota 10.21: Ryhmässä A_4 on 8 3-sykliä, joiden pitäisi edellä tehdyn laskun nojalla sisältyä kuuden alkion aliryhmään. Siis ryhmällä A_4 ei ole kuuden alkion aliryhmää.

Ryhmän A_4 aliryhmärakenne on seuraavan kaavion mukainen:



Mitkä tahansa kaksi ryhmän A_4 kertaluvun 2 alkioista $(12)(34)$, $(13)(24)$ ja $(14)(23)$ virittävät kaaviossa esiintyvän Kleinin neliryhmän K_4 . Esimerkiksi

$$(12)(34)(13)(24) = (14)(23) = (13)(24)(12)(34), \quad (12.1)$$

joten alkiot $(12)(34)$ ja $(13)(24)$ kommutoivat. Proposition 9.12 ja yhtälön (12.1) avulla näemme, että

$$\langle(12)(34)\rangle\langle(13)(24)\rangle = \langle(12)(34), (13)(24)\rangle = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

Siis $\langle(12)(34), (13)(24)\rangle$ on aliryhmien $\langle(12)(34)\rangle$ ja $\langle(13)(24)\rangle$ sisäinen suora tulo. Proposition 9.24 nojalla

$$\langle(12)(34), (13)(24)\rangle \cong \langle(12)(34)\rangle \times \langle(13)(24)\rangle \cong K_4.$$

12.4 Ryhmien toinen ja kolmas isomorfismilause

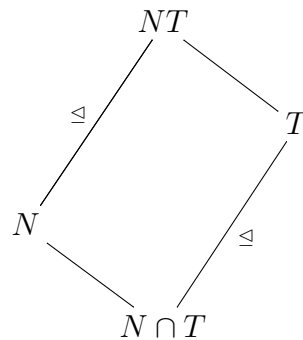
Ryhmien ensimmäisen isomorfismilauseen avulla todistetaan lisää tekijäryhmien isomorfisuustuloksia.

Propositio 12.22. *Olkoon G ryhmä ja olkoot $N \trianglelefteq G$ ja $T \leq G$. Tällöin*

$$NT = TN = \langle N \cup T \rangle \leq G.$$

Todistus. Harjoitustehtävä 12.13. □

Lause 12.23 (Ryhmien toinen isomorfismilause). *Olkoon G ryhmä. Olkoot $N, T \leq G$, $N \trianglelefteq G$. Tällöin $N \cap T \trianglelefteq T$ ja ryhmät $T/N \cap T$ ja NT/N ovat isomorfisia.*



Todistus. Olkoon $\pi: G \rightarrow G/N$ tekijäkuvaus. Koska $\ker \pi|_T = T \cap N$, Seurauksen 12.8 nojalla $T \cap N \trianglelefteq T$ ja ensimmäisen isomorfismilauseen nojalla pätee $T/N \cap T \cong \pi(T)$. Vastaavasti $\ker \pi|_{NT} = N$ ja koska kaikille $n \in N$ ja $t \in T$ pätee

$$\pi(nt) = ntN = tnN = \pi(t),$$

saadaan $\pi(NT) = \pi(T)$ ja ensimmäisen isomorfismilauseen nojalla

$$NT/N \cong \pi(T) \cong T/N \cap T. \quad \square$$

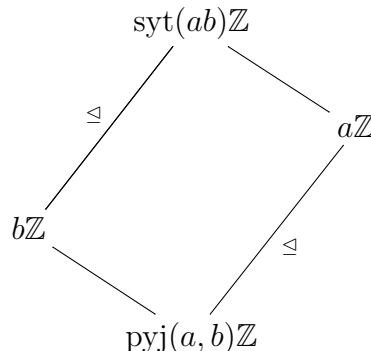
Seuraus 12.24. *Olkoot $a, b \in \mathbb{Z}$. Tällöin*

$$\text{syt}(a, b) \text{ pyj}(a, b) = ab.$$

Todistus. Toisen isomorfismilauseen nojalla tekijäryhmät $\text{syt}(ab)\mathbb{Z}/b\mathbb{Z} = \langle a, b \rangle / \langle b \rangle$ ja $\langle a \rangle / \langle a \rangle \cap \langle b \rangle = a\mathbb{Z} / \text{pyj}\mathbb{Z}$ ovat isomorfisia. Harjoitustehtävän 11.4 nojalla

$$\text{syt}(ab)/b = \# \text{syt}(ab)\mathbb{Z}/b\mathbb{Z} = \#a\mathbb{Z} / \text{pyj}\mathbb{Z} = a / \text{pyj}(a, b),$$

mistä väite seuraa. □



Lause 12.25 (Ryhmien kolmas isomorfismlause). *Olkoon G ryhmä. Olkoot $K \leq H \leq G$, $K, H \trianglelefteq G$. Tällöin ryhmät G/H ja $(G/K)/(H/K)$ ovat isomorfisia.*

Todistus. Osoitamme, että kuvaus $\phi: G/K \rightarrow G/H$, $\phi(xK) = xH$ on surjektiivinen homomorfismi, $\ker \phi = H/K$. Kuvaus on hyvin määritelty, koska $K \subset H$. Surjektiivisuus on selvää. Lisäksi

$$\phi(xKyK) = \phi(xyK) = xyH = xHyH = \phi(xK)\phi(yK),$$

joten kuvaus on homomorfismi. Lisäksi $\phi(yK) = yH = H$, kun $y \in H$, joten $H/K \subset \ker \phi$. Toisaalta, jos $y \notin H$, niin $yH \neq H$, joten $H/K = \ker \phi$. Väite seuraa isomorfismlauseesta 12.17. \square

Harjoitustehtäviä

12.1. Todista Propositio 12.7(2).

12.2. Olkoon $n \geq 2$. Osoita, että $\text{SO}(n) \trianglelefteq \text{O}(n)$. Onko $\text{O}(n) \triangleleft \text{GL}_n(\mathbb{R})$?²

12.3. (a) Osoita, että ryhmän G keskus $Z(G)$ on normaali aliryhmä.³

(b) Osoita, että ryhmän Q_8 kaikki aliryhmät ovat normaaleja.⁴

12.4. Osoita, että $Q_8/Z(Q_8) \cong K_4$.⁵

12.5. Olkoon $H \trianglelefteq A_n$ normaali aliryhmä, joka sisältää ainakin yhden 3-syklin. Osoita, että $H = A_n$.⁶

12.6. Olkoon G ryhmä, olkoon $I \neq \emptyset$ jokin indeksijoukko ja olkoot $H_i \trianglelefteq G$, $i \in I$. Osoita, että

$$\bigcap_{i \in I} H_i \trianglelefteq G.$$

12.7. Todista Propositio 12.16.

12.8. Osoita, että $\mathbb{C}^\times / \{-1, 1\} \cong \mathbb{C}^\times$.⁷

12.9. Osoita, että $\mathbb{C}^\times / \mathbb{R}_+ \cong \mathbb{S}^1$.

12.10. Olkoot $N_1 \trianglelefteq G_1$ ja $N_2 \trianglelefteq G_2$. Osoita, että $N_1 \times N_2 \trianglelefteq G_1 \times G_2$ ja

$$(G_1 \times G_2) / (N_1 \times N_2) \cong (G_1 / N_1) \times (G_2 / N_2).⁸$$

12.11. Olkoon H_3 3-ulotteinen Heisenbergin ryhmä.⁹ Olkoon $\psi: H_3 \rightarrow (\mathbb{R}^2, +)$,

$$\psi\left(\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}\right) = (a, b).$$

Osoita, että ψ on homomorfismi ja määritä sen ydin. Osoita, että $H_3 / \ker \psi \cong (\mathbb{R}^2, +)$.

²Tarkastele viimeisessä kysymyksessä ensin tapaus $n = 2$.

³Keskus määriteltiin Harjoitustehtävän 9.6 yhteydessä.

⁴ Q_8 määriteltiin Harjoitustehtävän 11.9 yhteydessä.

⁵Muodosta tekijäryhmän laskutaulu.

⁶Propositio 10.21 ja Harjoitustehtävä 10.11.

⁷Sovella ryhmien ensimmäistä isomorfismlauseetta.

⁸Sovella ryhmien ensimmäistä isomorfismlauseetta.

⁹Heisenbergin ryhmä määriteltiin Harjoitustehtävän 9.4 yhteydessä.

12.12. Olkoon C syklinen ryhmä. Osoita, että ryhmällä (\mathbb{S}^1, \cdot) on ryhmän C kanssa isomorfinen aliryhmä.¹⁰

12.13. Todista Propositio 12.22.¹¹

Olkoon G ryhmä. Alkioiden $a, b \in G$ **kommutaattori** on $[a, b] = aba^{-1}b^{-1}$. Ryhmän G **kommutaattorialiryhmä** $[G, G]$ on kaikkien kommutaattorien $[a, b]$, $a, b \in G$ virittämä aliryhmä

$$[G, G] = \langle [a, b] : a, b \in G \rangle.$$

12.14. Osoita, että $[G, G] \trianglelefteq G$.¹²

12.15. Osoita, että $G/[G, G]$ on kommutatiivinen ryhmä.

¹⁰Luvussa 9 tehtiin jotain hyödyllistä.

¹¹Riittää osoittaa, että $NT = TN$ on ryhmä, katso luku 9.5.

¹²Propositio 9.12. Laske ensin $[a, b]^{-1}$ ja osoita, että $g[a, b]g^{-1} \in [G, G]$ kaikilla $a, b, g \in G$.

Luku 13

Ryhmät ja geometria

Kurssin viimeisessä luvussa tarkastelemme säännöllisten monikulmioiden ja monitahokaiden symmetrioita abstraktin ryhmäteorian, lineaarialgebran ja symmetristen ryhmien avulla. Luvussa 9.6 tehdyn sopimuksen mukaisesti ajattelemme ortogonaaliryhmän $O(n)$ alkioita tarpeen mukaan joko ortogonaalisina $n \times n$ -matriiseina tai vastaavina lineaarikuvauksina.

13.1 Säännöllisten monikulmioiden symmetrioista

Luvussa 9.6 määritelty ortogonaaliryhmä $O(n)$ on tärkeä ryhmä euklidisessa geometriassa, sillä sen alkiot säilyttävät etäisyydet ja kulmat euklidisessa avaruudessa \mathbb{E}^n .¹ Tässä luvussa tarkastelemme ortogonaalimatriiseja, joita vastaavat kuvaukset kuvaavat 0-keskisen säännöllisen monikulmion itselleen. Palautamme ensin mieleen lineaarialgebrasta tunnettuja ortogonaalimatriiseja:

Esimerkki 13.1. (a) Matriisi

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O(2) - SO(2)$$

on lineaarikuvauksena **peilaus** $sx = (x_1, -x_2)$, joka kiinnittää pisteittäin ensimmäisen koordinaattiakselin $\mathbb{R} \times \{0\}$. Selvästi $\text{ord } s = 2$.

(b) Olkoon $\theta \in \mathbb{R}$. Matriisi

$$r_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \in SO(2)$$

on lineaarikuvauksena **kierto** kulman θ verran positiiviseen kiertosuuntaan. Jos n on positiivinen luonnollinen luku, niin selvästi $\text{ord } r_{2\pi/n} = n$.

Kaikille $\theta \in \mathbb{R}$ pätee

$$sr_\theta s = r_\theta^{-1} = r_{-\theta}.$$

¹Katso Lemma 9.28.

Lisäksi $r_\theta s r_\theta^{-1}$ on peilaus, joka kiinnittää pisteittäin suoran $r_\theta(\mathbb{R} \times \{0\})$.

Olkoon P_n säännöllinen n -kulmio euklidisessa tasossa \mathbb{E}^2 siten, että monikulmion P_n keskipiste on 0 ja yksi kärjistä on $(1, 0)$, kun $n \geq 3$ on luonnollinen luku. Ortogonaaliryhmän aliryhmä^a

$$D_n = \{A \in O(2) : AP_n = P_n\}$$

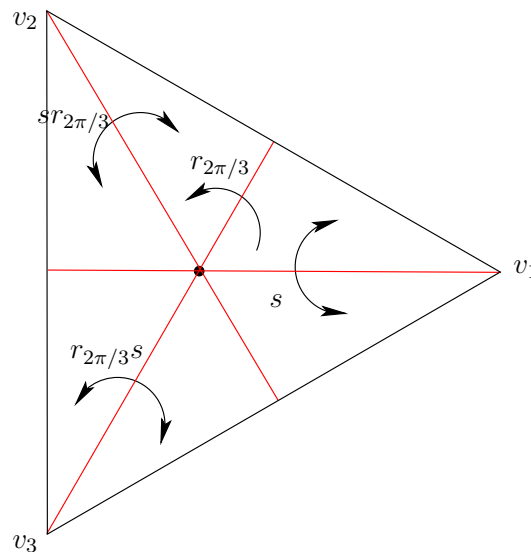
on **diedriryhmä** eli **kaksitahokasryhmä**.^b

^aKatso Harjoitustehtävä 13.1.

^bMerkintä AP_n tarkoittaa kuvajoukkoa $AP_n = \{Ax : x \in P_n\}$.

Euklidisen avaruuden \mathbb{E}^3 monitahokkaita voi kutsua myös kansainvälisemmällä nimellä polyedri, nelitahokastahan kutsutaankin useammin tetraedriksi, 8-tasokasta oktaedriksi ja niin edelleen. Jos ajatellaan monikulmio P_n upotettuna 3-ulotteiseen avaruuteen, sillä on yläpuoli ja alapuoli, joten monitahokkaana se on kaksitahokas.

Esimerkki 13.2. Kolmiolla P_3 on kuusi symmetriaa: identtinen kuvaus id , kierrot $r_{2\pi/3}$ ja $r_{2\pi/3}^2 = r_{-2\pi/3}$ ja peilaukset s , $r_{2\pi/3}s = r_{2\pi/3}^{-1}sr_{2\pi/3}$ ja $sr_{2\pi/3} = r_{2\pi/3}sr_{2\pi/3}^{-1}$ kunkin kärjen kautta kulkevien kulmanpuolittajasuorien suhteen.

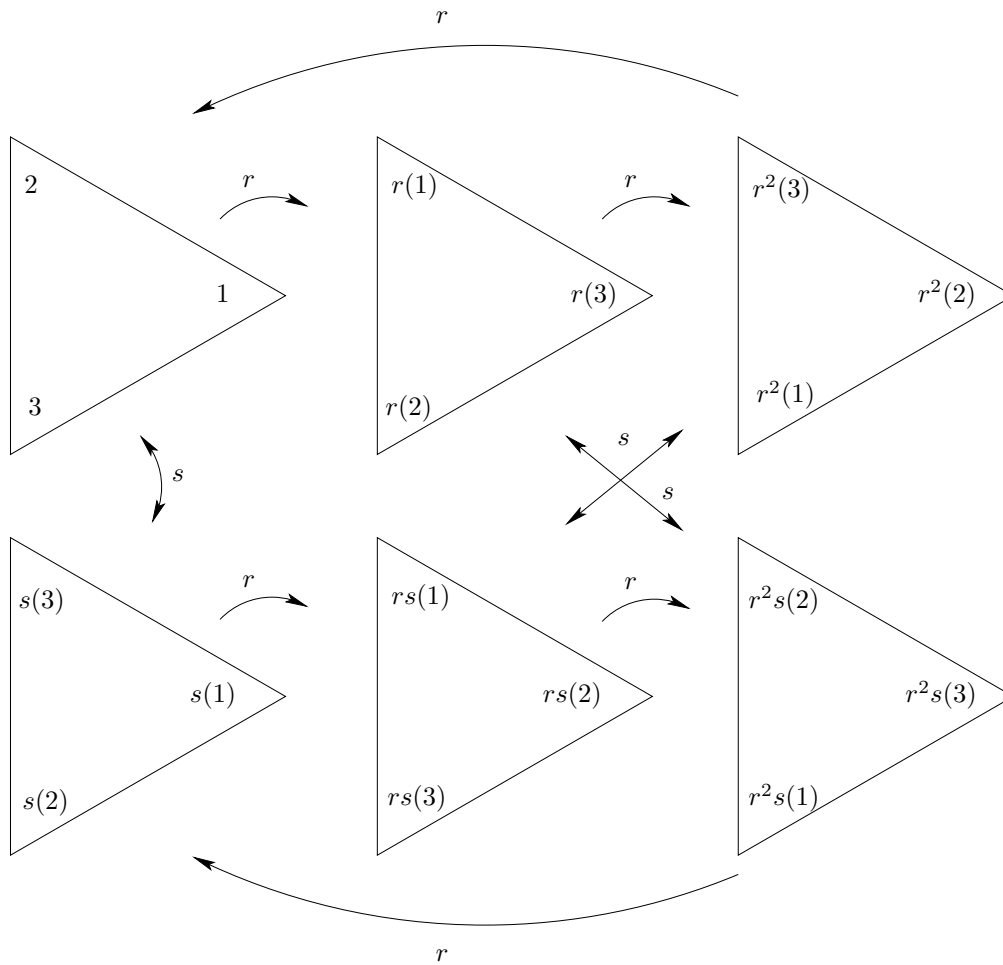


Kuva 131: Kolmion P_3 symmetrioita.

Jos kolmio P_3 ajatellaan kolmiulotteisessa avaruudessa \mathbb{E}^3 kaksipuolisena levynä, joka sisältyy tasoon $\mathbb{E}^2 \times \{0\}$, niin kuvaukset id , $r_{2\pi/3}$ ja $r_{2\pi/3}^2$ kuvaavat kolmion yläpuolen yläpuoleksi ja muut kuvaavat yläpuolen alapuoleksi.

Lemma 13.3. *Olkoon $n \geq 3$ luonnollinen luku. Tällöin*

- (1) $D_n \leq O(2)$.
- (2) $D_n = \langle s, r_{2\pi/n} \rangle$.
- (3) $\#D_n = 2n$.



Kuva 132: Ryhmän D_3 toiminta kolmiolla P_3 . Kuvassa $r = r_{2\pi/3}$ ja kärkiä v_1, v_2 ja v_3 on merkitty indekseillä 1, 2 ja 3.

Todistus. (1) Harjoitustehtävä 13.1.

(2) Osoitetaan ensin, että $\langle s, r_{2\pi/n} \rangle \leq D_n$: Olkoon

$$V_n = \{v_1 = (1, 0), v_2, \dots, v_n\}$$

monikulmion P_n kärkien joukko järjestettynä positiivisen kiertosuunnan mukaan. Matriisia $r_{2\pi/n}$ vastaava lineaarikuvaus kiertää monikulmiota P_n siten, että $r_{2\pi/n}v_j = v_{j+1}$, kun $1 \leq j \leq n-1$ ja $r_{2\pi/n}v_n = v_1$. Jos n on parillinen, niin s kiinnittää kärkipisteet v_1 ja $v_{\frac{n}{2}+1}$ ja $s(v_k) = v_{n+2-k}$ kaikille $2 \leq k \leq \frac{n}{2}$. Jos n on pariton, niin s kiinnittää vain kärjen v_1 ja $s(v_k) = v_{n+2-k}$ kaikille $2 \leq k \leq \frac{n+1}{2}$. Kaikki kuvaukset, joita saadaan yhdistettynä kuvauksina kuvauksista $r_{2\pi/n}^{\pm 1}$ ja $s = s^{-1}$ kuvaavat monikulmion P_n itselleen. Proposition 9.12 nojalla siis $\langle s, r_{2\pi/n} \rangle \leq D_n$.

Olkoon $f \in D_n$. Tällöin on $m \in \mathbb{Z}$ siten, että $sr_{2\pi/n}^m f(1, 0) = (1, 0)$ ja myös molemmat viereiset kärjet kuvautuvat itselleen. Tällöin $sr_{2\pi/n}^m f = \text{id}$, koska identtinen kuvaus on ainoa tason lineaarikuvaus, joka kiinnittää kaksi lineaarisesti riippumatonta vektoria. Siis $f \in \langle s, r_{2\pi/n} \rangle$, joten $D_n \leq \langle s, r_{2\pi/n} \rangle$.

(3) Kuvaus $d \in D_n$ määräytyy yksikäsitteisesti, kun valitaan, mihin n eri vaihtoehdosta kärkipiste $(1, 0)$ kuvautuu ja valitaan, vaihtuuko kärkien kiertosuunta kuvauksessa d vai ei (kaksi vaihtoehtoa). Siis $\#D_n = 2n$. \square

Diedriryhmän D_n **permutaatioesitys** on kuvaus $\rho_n: D_n \rightarrow S_n$, joka määritellään siten, että alkioita $A \in D_n$ vastaa permutaatio $\rho_n(A) \in S_n$, jolle pätee

$$Av_k = v_{\rho_n(A)(k)} \quad (13.1)$$

kaikille $k \in \{1, 2, \dots, n\}$.

Lemman 13.3(2) todistuksessa näimme, että

$$\rho_n(r_{2\pi/n}) = (12 \cdots n).$$

Permutaation ρ_n lauseke riippuu siitä, onko n parillinen vai pariton: Parillisille n pätee

$$\rho_n(s) = (2n)(3(n-1)) \cdots \left(\frac{n}{2} \frac{n}{2} + 2\right) = \prod_{k=2}^{\frac{n}{2}} (k(n-k+2)) \quad (13.2)$$

ja parittomille pätee

$$\rho_n(s) = (2n)(3(n-1)) \cdots \left(\frac{n+1}{2} \frac{n+1}{2} + 2\right) = \prod_{k=2}^{\frac{n+1}{2}} (k(n-k+2)). \quad (13.3)$$

Propositio 13.4. *Kuvaus ρ_n on uskollinen esitys.*

Todistus. Lemman 13.3 todistuksessa näimme, että lineaarikuvauksen $A \in D_n$ rajoittuma monikulmion P_n joukkoon V_n määrää symmetrisen ryhmän $\text{Perm}(V_n) \cong S_n$ alkion $\rho(A)$ yhtälön (13.1) mukaisesti. Olkoot $A, B \in D_n$. Tällöin kaikille $k \in \{1, 2, \dots, n\}$ pätee

$$v_{\rho_n(AB)} = (AB)v_k = A(Bv_k) = Av_{\rho_n(B)(k)} = v_{\rho_n(A)(\rho_n(B)(k))} = v_{\rho_n(A)(\rho_n(B)(k))},$$

joten ρ_n on homomorfismi. Se on injektiivinen Lemman 13.3(2) todistuksen loppuosan ja Proposition 9.9 nojalla. \square

Seuraus 13.5. $D_n \cong \langle \rho_n(r_{2\pi/n}), \rho_n(s) \rangle \cong \langle (1, 2, \dots, n), \rho_n(s) \rangle \leq S_n$. \square

Homomorfismi ρ_n ei ole surjektio, kun $n \geq 4$, koska tällöin $\#D_n = 2n < n! = \#S_n$.

Esimerkki 13.6. Ryhmä D_3 on isomorfinen ryhmän S_3 kanssa, koska homomorfismi $\rho_3: D_3 \rightarrow S_3$ on injektio ja $\#D_3 = 6 = \#S_3$. Yhtälön (13.3) mukaan $\rho_3(s) = (23)$.

Esimerkki 13.7. Lemman 13.3 nojalla neljän diedriryhmä on

$$D_4 = \langle r_{\pi/2}, s \rangle = \left\langle \left(\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \right\rangle.$$

Diedriryhmässä D_4 on 8 alkioita: Neutraalialkion I_2 , lisäksi on kierrot

$$r_{\pi/2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{ja} \quad r_{\pi/2}^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

joiden kertaluku on 4, ja viisi kertaluvun 2 alkioita $r_{\pi/2}^2 = -I_2 \in Z(D_4)$, s ,

$$r_{\pi/2} s r_{\pi/2}^{-1} = s r_{\pi/2}^2 = -s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$r_{\pi/2} s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{ja} \quad s r_{\pi/2} = -r_{\pi/2} s = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

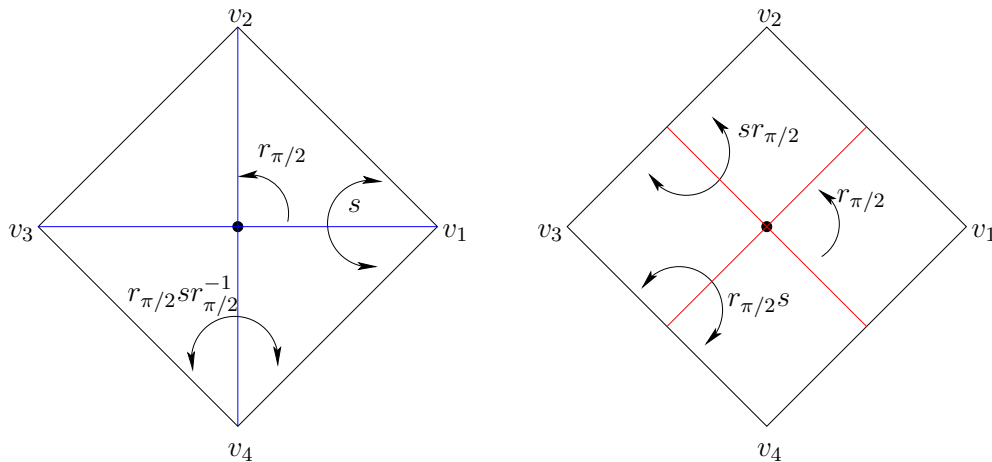
Lagrangen lauseen nojalla tai virittäjiä tarkastelemalla nähdään, että

$$\langle r_{\pi/2}, s \rangle = \langle r_{\pi/2}, s r_{\pi/2} \rangle = \langle r_{\pi/2}, r_{\pi/2} s \rangle = \langle r_{\pi/2}, r_{\pi/2} s \rangle = D_4.$$

Samoin virittäjistä näkee helposti, että

$$\langle s, r_{\pi/2} s \rangle = \langle s, s r_{\pi/2} \rangle = \langle s r_{\pi/2}^2, r_{\pi/2} s \rangle = \langle s r_{\pi/2}^2, s r_{\pi/2} \rangle = \langle s, r_{\pi/2} \rangle = D_4,$$

joten kertaluvun 4 alkioit esiintyvät vain syklisessä aliryhmässä $\langle r_{\pi/2} \rangle$ ja koko ryhmässä D_4 . Kertaluvun 2 alkioit virittävät kukin kahden alkion syklisen ryhmän, joita on siis viisi.



Kuva 133: Ryhmällä D_4 on kaksi aliryhmää, jotka ovat Kleinin neliryhmiä.

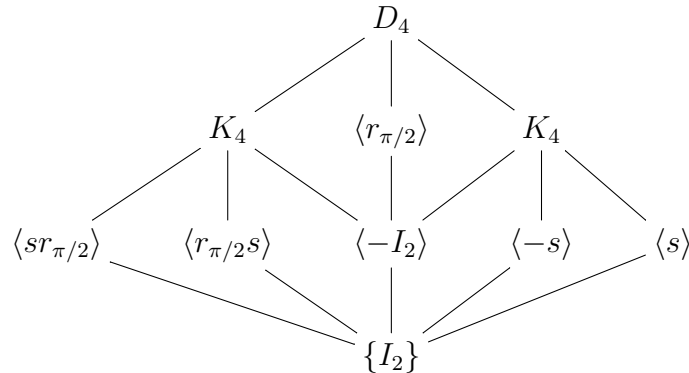
Lisäksi on helppo tarkastaa, että

$$\langle -I_2, s \rangle = \langle -I_2, -s \rangle = \langle s, -s \rangle = \{I_2, -I_2, s, -s\}.$$

Koska $-I_2$ on keskuksessa, tämä ryhmä on Kleinin neliryhmä. Vastaavalla tavalla nähdään, että

$$\langle -I_2, r_{\pi/2} s \rangle = \langle -I_2, s r_{\pi/2} \rangle = \langle r_{\pi/2} s, s r_{\pi/2} \rangle = \{I_2, -I_2, r_{\pi/2} s, s r_{\pi/2}\} \cong K_4.$$

Ryhmän D_4 aliryhmäkaavio on siis



Kleinin neliryhmän kanssa isomorfiset aliryhmät koostuvat identtisen kuvauksen lisäksi kahdesta keskenään kohtisuorien akselien suhteen tehtävästä peilauksesta ja niiden yhdistettynä kuvauksena saatavasta kierrosta $-I_2$, katso Kuva 133.

Yhtälön (13.2) mukaan $\rho_4(s) = (24)$ ja Seurauksen 13.5 nojalla diedriryhmä D_4 on isomorfinen ryhmän $\langle (1234), (24) \rangle < S_4$ kanssa.

Seuraava tulos osoittaa, että se, että valitsimme monikulmion P_n yhdeksi kärjeksi pisteen $(0, 1)$ ei ole oleellista.

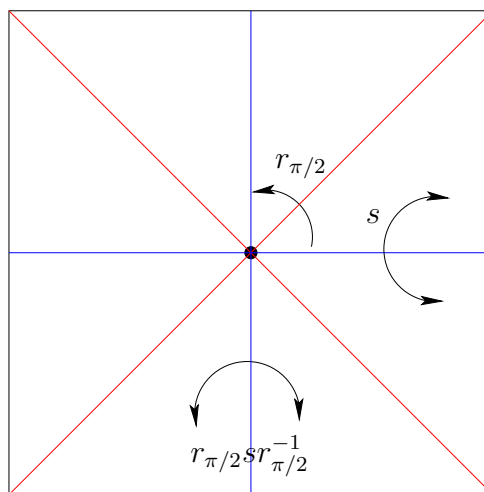
Lemma 13.8. *Olkoon $n \geq 3$, olkoon $\theta \in \mathbb{R}$ ja olkoon $P_n^\theta = r_\theta(P_n)$. Ryhmät D_n ja $\{A \in O(2) : AP_n^\theta = P_n^\theta\}$ ovat isomorfiset.*

Todistus. Harjoitustehtävä 13.2. □

Esimerkki 13.9. Olkoon

$$P_4^{\pi/4} = r_{\pi/4}(P_4) = \{x \in \mathbb{R}^2 : |x_1| \leq 1, |x_2| \leq 1\}.$$

Proposition 13.8 nojalla ryhmät $\{A \in O(2) : AP_n^\theta = P_n^\theta\}$ ovat isomorfisia. Itse asiassa tässä tapauksessa pätee jopa yhtälö $D_4 = \{A \in O(2) : AP_n^\theta = P_n^\theta\}$.



Kuva 134: Ryhmän D_4 alkioita kierretyn neliön symmetrioina.

13.2 Monitahokkaiden symmetrioista

Esimerkki 13.10. Kolmiulotteisen avaruuden erityisen ortogonaaliryhmän $SO(3)$ neutraalialkiosta poikkeavat alkiot vastaavat avaruuden \mathbb{R}^3 kiertoja jonkin (origon kautta kulkevan) suoran ympäri. Esimerkiksi matriisi

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SO(3)$$

on kierto kulman $\theta \in \mathbb{R}$ verran kolmannen koordinaattiakselin ympäri.

Olkoon $K \subset \mathbb{R}^3$ kuutio, jonka kärkipisteiden joukko on

$$V_K = \{(\varepsilon_1, \varepsilon_2, \varepsilon_3) : \varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{-1, 1\}\}.$$

Kuution K **symmetriaryhmä** on

$$\Gamma_K = \{A \in O(3) : AK = K\}$$

ja sen **kiertosymmetriaryhmä** on

$$\Gamma_K^+ = \{A \in SO(3) : AK = K\}$$

Kuten luvussa 13.1 nähdään helposti, että ryhmät Γ_K ja Γ_K^+ ovat isomorfisia joidenkin ryhmän $\text{Perm}(V_K) \cong S_8$ aliryhmien kanssa. Tässä luvussa tarkastelemme ryhmien Γ_K ja Γ_K^+ toimintaa pienemmällä joukolla ja saamme näiden ryhmien rakenteen selvitettyä täydellisesti.

Propositio 13.11. $\Gamma_K^+ \cong S_4$.

Todistus. Olkoon

$$H = \{\{v, -v\} : v \in V_K\}.$$

Joukko $H = \{h_1, h_2, h_3, h_4\}$ koostuu kuution K vastakkaisten kärkipisteiden muodostamista joukon V osajoukoista, joita voi ajatella kuution neljänä lävistäjänä.

Määritellään ryhmän Γ_K toiminta $\rho_0: \Gamma_K \rightarrow \text{Perm}(H) \cong S_4$ joukolla H asettamalla

$$\rho_0(g)(\{v, -v\}) = \{gv, g(-v)\} = \{gv, -gv\}$$

kaikilla $g \in \Gamma_K$ ja $v \in V$. Näin saamme ryhmän Γ_K toiminnan ρ joukolla $\{1, 2, 3, 4\}$ määrittelemällä, että $\rho(g) \in S_4$ on se permutaatio, jolle pätee $\rho_0(g)(h_k) = h_{\rho(g)(k)}$ kaikilla $k \in \{1, 2, \dots, n\}$.

Kuution K kärjet virittävät vektoriavaruuden \mathbb{R}^3 , joten $\{gv, -gv\} = \{g'v, -g'v\}$ kaikille $v \in V_K$, jos ja vain jos $g' = \pm g$, joten $\ker \rho = \{-\text{id}, \text{id}\}$. Lisäksi $\ker \rho \cap \Gamma_K^+ = \{\text{id}\}$, joten $\rho|_{\Gamma_K^+}$ on uskollinen esitys. Harjoitustehtävässä 13.3 osoitetaan, että $\rho|_{\Gamma_K^+}: \Gamma_K^+ \rightarrow S_4$ on surjektio. \square

Propositio 13.12. $\Gamma_K \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$.

Todistus. Olkoon $\rho: \Gamma_K \rightarrow s_4$ kuten Proposition 13.11 todistuksessa, jossa näimme, että $\ker \rho = \{\text{id}, -\text{id}\} \leq Z(\Gamma_K)$. Kaikille $A \in \Gamma_K^+$ pätee määritelmän nojalla $\det A = 1$. Koska $\det(-\text{id}) = -1$ on siis $-\text{id} \in \Gamma_K - \Gamma_K^+$. Siis $\langle \Gamma_K^+, \ker \rho \rangle \geq \#\Gamma_K^+ + 1$ ja koska $[\Gamma_K : \Gamma_K^+] = 2$, niin Lagrangen lauseen nojalla $\langle \Gamma_K^+, \ker \rho \rangle = \Gamma_K$. Propositioiden 9.24 ja 8.18(4) nojalla

$$\Gamma_K \cong \Gamma_K^+ \times \ker \rho \cong \Gamma_K^+ \times (\mathbb{Z}/2\mathbb{Z}). \quad \square$$

Kuution K kärkipisteiden joukon V_K osajoukko

$$V_T = \{(1, 1, 1), (1, -1, -1), (-1, 1, -1), (-1, -1, 1)\}$$

on säännöllisen tetraedrin T kärkipisteiden joukko. Tetraedrin T sivut ovat yhtä pitkiä keskenään ja kaikki tahot ovat tasasivuisia kolmioita. Tällä tavalla muodostetun tetraedrin painopiste on 0.

Tetraedrin T **symmetriaryhmä** on

$$\Gamma_T = \{A \in O(3) : AT = T\}$$

ja sen **kiertosymmetriaryhmä** on

$$\Gamma_T^+ = \{A \in SO(3) : AT = T\}.$$

Propositio 13.13. $\Gamma_T^+ \cong A_4$.

Todistus. On helppo tarkastaa, että $V_K = V_T \sqcup -V_T$, $\Gamma_T^+ \leq \Gamma_K^+$ ja että $gV_T = V_T$ tai $gV_T = -V_T$ kaikille $g \in \Gamma_K$. Olkoon $h \in H$. Jos $g \in \Gamma_K^+ - \{\text{id}\}$ on kierto akselin h määräämän akselin ympäri, niin g kuvaa tetraedrin T itselleen ja $\rho g \in \text{Perm } H$ on 3-sykli. Aliryhmä $\rho(\Gamma_T^+) \leq S_4$ sisältää ryhmän S_4 kaikki 8 3-sykliä, joten Proposition 10.21 nojalla $A_4 \leq \rho(\Gamma_T^+)$. Lagrangen lauseen nojalla $\#\Gamma_T^+ \in \{12 = \#A_4, 24\}$. Väite seuraa, koska $\Gamma_T^+ < \Gamma_K^+$. \square

Vastaavaan tapaan voidaan osoittaa, että ikosaedrin ja dodekaedrin kiertosymmetriaryhmä on isomorfinen ryhmän A_5 kanssa ja että näiden monitahokkaiden symmetriaryhmä on isomorfinen ryhmän $A_5 \times \mathbb{Z}/2\mathbb{Z}$ kanssa. Lisää tästä aihepiiristä voi lukea esimerkiksi lähteistä [Arm, luku 8] ja [Ber, luku 12.5].

Harjoitustehtäviä

13.1. Olkoon $n \geq 3$ luonnollinen luku. Osoita, että $D_n \leq O(2)$.

13.2. Todista Lemma 13.8.²

13.3. Osoita, että Proposition 13.11 todistuksessa käytettävä homomorfismi $\rho|_{\Gamma_K^+}$ on surjektio.³

²Mikä on *luonnollinen* kuvaus väitteen ryhmien välillä?

³Mieti tilannetta geometrisesti ja osoita, että ryhmässä Γ_K^+ on riittävän monta alkioita.

Olkoon $A \in O(n)$ ja olkoon $b \in \mathbb{R}^n$. Olkoon $E_{A,b}: \mathbb{R}^n \rightarrow \mathbb{R}^n$,

$$E_{A,b}(x) = Ax + b$$

kaikilla $x \in \mathbb{R}^n$. Joukko

$$E(n) = \{E_{A,b} : A \in O(n), b \in \mathbb{R}^n\}$$

varustettuna kuvausten yhdistämisellä on n -ulotteisen avaruuden **Eukleideen ryhmä**. Eukleideen ryhmän aliryhmä

$$T(n) = \{E_{I_n,b} \in E(n) : b \in \mathbb{R}^n\}$$

on n -ulotteisen avaruuden **siirtojen ryhmä**.

13.4. Osoita, että $E(n)$ on ryhmä.⁴

Olkoon H ryhmän G aliryhmä ja N ryhmän G normaali aliryhmä siten, että $G = NH$, Jos $N \triangleleft G$ ja $N \cap H = \{\text{id}\}$. Tällöin G on ryhmien N ja H **sisäinen puolisuora tulo**, jolloin käytetään merkintää $G = N \rtimes H$.^a

Jos $\tilde{N} \cong N$ ja $\tilde{H} \cong H$ ja $G = N \rtimes H$, niin G on ryhmien \tilde{N} ja \tilde{H} **(abstrakti) puolisuora tulo**, $G \cong \tilde{N} \rtimes \tilde{H}$.

^aMerkintä ei ole symmetrinen. Merkki \rtimes sisältää normaalin aliryhmän merkin \triangleleft . Muistisääntö auttaa: $N \triangleleft N \rtimes H$, siis kolmiot ovat samoin päin merkeissä \triangleleft ja \rtimes .

13.5. Osoita, että $T(n) \triangleleft E(n)$ ja että $E(n)/T(n) \cong O(n)$ ja että $E(n) = T(n) \rtimes O(n)$.

13.6. Osoita, että $O(n)$ ei ole ryhmän $E(n)$ normaali aliryhmä.

13.7. Osoita, että S_n on ryhmien A_n ja $\mathbb{Z}/2\mathbb{Z}$ puolisuora tulo.

⁴Kätevintä lienee osoittaa, että $E(n) \leq \text{Perm}(\mathbb{R}^n)$

Liite A

Kokonaislukujen jaollisuus

Tarkastelemme tässä luvussa lyhyesti jaollisuutta kokonaislukujen renkaassa \mathbb{Z} . Tulokset lienevät tuttuja niille, jotka ovat suorittaneet kurssin Lukuteoria 1. Muutama tulos, jonka todistus antaa mallia algebrallisen yleistyksensä todistukselle, todistetaan tässä liitteessä, muiden osalta viitataan kurssin Lukuteoria 1 luentoihin tai hyviin lukuteorian kirjoihin kuten [JJ].

Propositio A.1 (Jakoyhtälö). *Olkoot $a \in \mathbb{N} - \{0\}$ ja $b \in \mathbb{Z}$. Tällöin on yksikäsitteiset $q, r \in \mathbb{Z}$ siten, että*

$$b = qa + r \quad \text{ja} \quad 0 \leq r < a.$$

Todistus. Olkoon

$$S = \{b - ka : k \in \mathbb{Z}\} \cap \mathbb{N}.$$

Joukko S ei ole tyhjä, koska $b - (-b^2) \cdot a = b + b^2 a \geq 0$ kaikille $b \in \mathbb{Z}$ ja kaikille $a > 0$. Koska S on luonnollisten lukujen epätyhjä osajoukko, niin sillä on pienin alkio. Määritelmän nojalla $\min S = b - qa$ jollakin $q \in \mathbb{Z}$. Jos $\min S \geq a > 0$, niin $b - (q+1)a = \min S - a \geq 0$, joten $\min S - a \in S$. Tämä on mahdotonta, joten $\min S < a$. Väitteen olemassaolotulos seuraa valitsemalla $r = \min S$.

Oletetaan, että on $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1, r_2 < a$, joille

$$b = q_1 a + r_1 = q_2 a + r_2.$$

Tällöin $(q_1 - q_2)a = r_2 - r_1$. Jos $q_1 \neq q_2$, niin $|q_1 - q_2| \geq 1$ ja siten $|r_2 - r_1| \geq a$. Tämä on mahdotonta, sillä $0 \leq r_1, r_2 \leq a - 1$. Täytyy siis olla $q_1 = q_2$ ja siten myös $r_1 = r_2$. \square

Jos $a, b, c \in \mathbb{Z}$ siten, että $ab = c$, niin a ja b ovat luvun c tekijöitä. Tällöin luvut a ja b jakavat luvun c , mistä käytetään merkintää $a \mid c$ ja vastaavasti $b \mid c$.

Jos luku $d \in \mathbb{Z}$ jakaa kokonaisluvut a ja b , niin d on lukujen a ja b yhteinen tekijä.

Jos $m, n \in \mathbb{Z}$ ja $d \in \mathbb{N}$ on lukujen m ja n yhteinen tekijä, jonka jokainen lukujen m ja n yhteinen tekijä jakaa, niin d on lukujen m ja n suurin yhteinen tekijä, merkitään $d = \text{syt}(m, n)$.

Jos $\text{syt}(m, n) = 1$, sanotaan, että luvut m ja n ovat suhteellisia alkulukuja ja että m ja n ovat keskenään jaottomia.

Esimerkki A.2. Luvun 12 tekijät ovat $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$ ja ± 12 . Luvun 30 tekijät ovat $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15$ ja ± 30 , joten lukujen 12 ja 30 yhteiset tekijät ovat $\pm 1, \pm 2, \pm 3$ ja ± 6 ja $\text{syt}(12, 30) = 6$.

Propositio A.3 (Bezout'n yhtälö). Olkoot $a, b \in \mathbb{Z}$. Yhtälöllä

$$xa + yb = n$$

on kokonaislukuratkaisu $(x, y) \in \mathbb{Z}^2$, jos ja vain jos $\text{syt}(a, b) \mid n$.

Todistus. Tämä tulos todistetaan lukuteorian alkeiskursseilla jakoyhtälön avulla. □

Propositio A.4. Olkoot $a, b \in \mathbb{Z}$ keskenään jaottomia ja $c \in \mathbb{Z}$. Tällöin

(1) Jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$.

(2) Jos $a \mid bc$, niin $a \mid c$.

Todistus. (1) Koska $\text{syt}(a, b) = 1$, niin $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$. Oletuksen nojalla on $k, l \in \mathbb{Z}$ siten, että $ka = c = lb$. Nyt on

$$c = c(xa + yb) = cxa + cyb = (lb)xa + (ka)yb = ab(lx + ky)$$

ja $lx + ky \in \mathbb{Z}$, joten $ab \mid c$.

(2) Kuten kohdassa (1) saadaan $c = cxa + cyb$ jollain $x, y \in \mathbb{Z}$. Koska $a \mid bc$ ja $a \mid a$, niin a jakaa summan $cxa + ybc = c$. □

Luonnollinen luku $p \geq 2$ on alkuluku, jos kaikille $a, b \in \mathbb{N}$ pätee $p \mid a$ tai $p \mid b$, jos $p \mid ab$.

Luonnollinen luku $p \geq 2$ on jaoton, jos ehdosta $p = ab$ luonnollisilla luvuilla a, b seuraa $a = 1$ tai $b = 1$

Propositio A.5. Jaottomat luvut ovat alkulukuja.

Todistus. Olkoon p alkuluku. Oletetaan, että $p = ab$. Riittää tarkastella tapaus $p \mid a$. Tällöin $a = pc$ jollakin $c \in \mathbb{N}$, joten $p = pcb$. Supistamalla p molemmilta puolilta saadaan, $pc = 1$, joten $p = 1$. Siis p on jaoton. □

Propositio A.6 (Eukleideen lemma). Alkuluvut ovat jaottomia.

Todistus. Olkoon $p \in \mathbb{Z}$ jaoton ja olkoot $a, b \in \mathbb{Z}$ siten, että p on luvun ab tekijä. Oletetaan, että p ei jaa lukua a . Tällöin $\text{syt}(a, p) = 1$, joten väite seuraa Proposition A.4 kohdasta (2). □

Lause A.7 (Aritmetiikan peruslause). *Jokainen nollasta poikkeava kokonaisluku $q \in \mathbb{Z} - \{0\}$ voidaan esittää positiivisten alkulukujen äärellisenä tulona muodossa*

$$q = (-1)^{m(q)} \prod_p p^{a_p(q)},$$

missä $m(q) \in \{0, 1\}$ ja $a_p(q) \in \mathbb{N}$ kaikille alkuluville $p \geq 2$. Tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.

Todistus. Tämä tulos todistetaan lukuteorian alkeiskursseilla. □

Aritmetiikan peruslauseen antamaa luvun $q \in \mathbb{Z} - \{0\}$, esitystä alkulukujen tulona sanotaan luvun q **alkutekijäesitykseksi**.

Alkuluvut p , joille $a_p(q) \neq 0$, ovat luvun q **alkutekijöitä**.

Kirjallisuutta

- [Arm] M. A. Armstrong. Groups and symmetry. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1988.
- [Ber] M. Berger. Geometry I-II. Universitext. Springer-Verlag, Berlin, 1987. Translated from the French by M. Cole and S. Levy.
- [DF] D. S. Dummit and R. M. Foote. Abstract algebra. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.
- [Gre] W. Greub. Linear algebra. Springer-Verlag, New York, fourth edition, 1975. Graduate Texts in Mathematics, No. 23.
- [Ham] G. Hamel. Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung: $f(x + y) = f(x) + f(y)$. Math. Ann., 60(3):459–462, 1905.
- [IR] K. Ireland and M. Rosen. A classical introduction to modern number theory, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990.
- [JJ] G. A. Jones and J. M. Jones. Elementary number theory. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 1998.
- [War] S. Warner. Modern algebra. Vols. I, II. Prentice-Hall Inc., Englewood Cliffs, N.J., 1965.